MATEMÁTICA ESTRUCTURAL

ANDRÉS FORERO CUERVO

MATEMÁTICA ESTRUCTURAL

Universidad de los Andes
Bogotá, DC
2009

Forero Cuervo, Andrés
Matemática estructural / Andrés Forero Cuervo. – Bogotá: Universidad de los Andes, Facultad de Ciencias, Departamento de Matemáticas, Ediciones Uniandes, 2009.
p. 344; 170 x 240 cm.

ISBN 978-958-695-452-5
1. Matemáticas - Fundamentos 2. Matemáticas – Enseñanza superior 3. Lógica simbólica y matemática – Enseñanza superior I. Universidad de los Andes (Colombia). Facultad de Ciencias. Departamento de Matemáticas II. Tít.

CDD 510.711 SBUA

© Andrés Forero Cuervo
aforeroc@uci.edu

© Universidad de los Andes
Facultad de Ciencias
Departamento de Matemáticas
Dirección: Carrera 1ª N° 18A-10
Teléfono: 3 32 43 40
Bogotá DC, Colombia

Ediciones Uniandes
Carrera 1ª N° 19-27, edificio AU 6
Bogotá DC, Colombia
Teléfono: 3 39 49 49 – 3 39 49 99, ext. 2133. Fax: ext. 2158
http//:libreria.uniandes.edu.co
infeduni@uniandes.edu.co

ISBN: 978-958-695-452-5

Edición, diseño gráfico, diagramación y tipografía: Nicolás Vaughan

Ilustraciones de carátula e interiores: Andrea Solano
andresoli3@yahoo.com

Diseño de la carátula: Juan David Martín

Impresión y acabados: Editorial Kimpres Ltda.
Dirección: Calle 16 sur N° 69C-17
Bogotá DC, Colombia
Teléfono: 4 13 68 84. Fax: 2 90 75 39

Impreso en Colombia – Printed in Colombia

Todos los derechos reservados. Esta publicación no puede ser reproducida ni en su todo ni en sus partes, ni registrada en o trasmitida por un sistema de recuperación de información, en ninguna forma ni por ningún medio sea mecánico, fotoquímico, electrónico, magnético, electro-óptico, por fotocopia o cualquier otro, sin el permiso previo por escrito de la editorial.

A Alejandro

Índice

Introducción **xi**

Agradecimientos **xvii**

1 Conjuntos **1**
1.1. Conceptos fundamentales 2
1.2. Propiedades de la relación $\subseteq$ y el conjunto potencia 15
1.3. Operaciones básicas entre conjuntos 23
1.4. Álgebra de conjuntos: pruebas sin doble inclusión 41
1.5. Unión e intersección generalizadas 48
1.6. Producto cartesiano 55
Proyecto 61
Lecturas adicionales 63

2 Inducción: los números naturales **65**
2.1. El Principio del Buen Orden 66
2.2. Demostraciones por inducción 71
2.3. Definiciones por recursión 83
2.4. Isomorfismos entre estructuras ordenadas 90
2.5. Conteo mediante inducción 95
Proyecto 103
Lecturas adicionales 108

3 Divisibilidad: los números enteros **109**
3.1. Conceptos fundamentales y el Algoritmo de la División 110
3.2. El máximo común divisor 115
3.3. El Teorema Fundamental de la Aritmética 124
3.4. Sucesiones finalmente nulas y el TFA 132
3.5. Congruencias y el Pequeño Teorema de Fermat 138
3.6. El Teorema Chino del Residuo 151
Proyecto 161
Lecturas adicionales 164

4 Relaciones y funciones **165**
4.1. Relaciones 166
4.2. Clausura de una relación 179
4.3. Funciones 186

4.4. Relaciones de equivalencia 205
4.5. Construcción de los números enteros y los racionales 222
4.6. Conteo mediante relaciones de equivalencia 234
Proyecto 240
Lecturas adicionales 242

5 Cardinales 243
5.1. Conceptos fundamentales 243
5.2. El Teorema de Cantor-Schröder-Bernstein 248
5.3. Conjuntos finitos 252
5.4. Conjuntos enumerables 255
5.5. Conjuntos infinitos no enumerables 264
Proyecto 270
Lecturas adicionales 272

6 Estructuras matemáticas 275
6.1. Conceptos fundamentales 276
6.2. Grupos 283
6.3. Isomorfismos entre estructuras 288
Proyecto 293
Lecturas adicionales 295

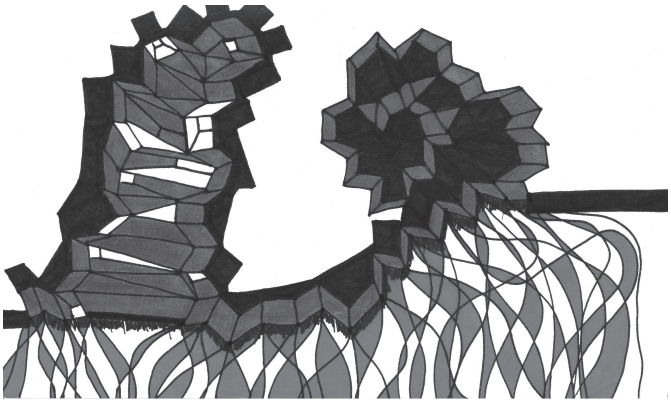
A Lógica 297
A.1. Lógica proposicional 297
A.2. La implicación 301
A.3. Demostraciones 302
A.4. Lógica de predicados 306

Bibliografía 313

Índice analítico 315

Índice de símbolos 321

INTRODUCCIÓN



Este libro constituye una introducción rigurosa a las matemáticas, partiendo del estudio de los conjuntos como pilar fundamental. Se cubren diversos temas como la teoría intuitiva de conjuntos, la inducción matemática, el conteo, la divisibilidad y las congruencias, las relaciones y funciones, los órdenes, las relaciones de equivalencia y la relación de equipotencia entre conjuntos. Además, se introduce el concepto de isomorfismo, noción que formaliza la idea de similitud estructural.

Este libro está dirigido a aquellos estudiantes universitarios que comienzan su carrera de matemática pura, y desean aprender a demostrar de manera rigurosa proposiciones matemáticas y entender los conceptos básicos que fundamentan el desarrollo de la matemática moderna. Sin embargo, el texto también puede ser utilizado en otros contextos como, por ejemplo, en cursos de matemáticas discretas para estudiantes de economía, física o ingenierías, o en los últimos cursos de aquellos colegios que prioricen la enseñanza significativa y rigurosa de las matemáticas.

Además de esto, el autor ofrece el libro a aquellos "matemáticos frustrados" que siempre quisieron profundizar más en la reina de las ciencias y que por diversas razones no han podido hacerlo. Este libro pretende ser para ellos la puerta de entrada definitiva al universo de los patrones y las estructuras.

Prerrequisitos

Esperamos que el lector esté familiarizado con temas matemáticos básicos de la escuela secundaria como, por ejemplo, aritmética, fracciones, valor absoluto, álgebra y factorización. No se necesitan nociones de geometría, trigonometría, álgebra lineal ni cálculo infinitesimal para leer este libro. Tampoco se requiere que el lector sepa hacer demostraciones matemáticas; precisamente uno de los objetivos del texto es enseñar ello al estudiante. Sin embargo, para facilitar esta tarea, se espera que el lector tenga un dominio de ciertas nociones básicas de lógica como, por ejemplo, tablas de verdad, conectivos proposicionales, cuantificadores —existencial y universal—, propiedades lógicas, teorema, hipótesis, conclusión, equivalencias y simbolización lógica. Por ello hemos incluido un apéndice al final del texto, el cual incluye varios ejercicios con los cuales el lector podrá familiarizarse en dichos temas.

Lógica

Se espera que el lector tenga un dominio de algunas nociones básicas de lógica proposicional para comprender este texto. Para asegurarse de que este sea el caso, recomendamos fuertemente que el lector estudie el Apéndice A que se incluye al final, antes de comenzar la lectura de los capítulos.

Vale aclarar que este libro *no* consiste en un estudio sobre lógica formal o lógica matemática; la lógica será utilizada a lo largo de él como una herramienta básica para entender y deducir proposiciones matemáticas.[1]

Lectura del texto

Es recomendable una lectura ordenada y completa de todos los capítulos del texto. Sin embargo, según las necesidades o intereses del estudiante, o del instructor que diseñe un curso de matemáticas que utilice este texto como guía, es posible prescindir del estudio de algunas de las partes de este texto. En particular, el autor considera que las siguientes secciones *no* son estrictamente esenciales para un entendimiento básico del tema: 1.5, 1.7, 2.5, 2.6, 3.4, 3.6, 3.7, 4.2, 4.5, 4.6, 4.7, 5.6 y 6.2.

A continuación se describirán brevemente los temas tratados en los diferentes capítulos de este texto:

[1] A quien esté interesado en un estudio de la lógica matemática, le recomendamos consultar [1]. (La bibliografía la encontrará el lector al final de este libro.)

Capítulo 1: Conjuntos

Estudiaremos las nociones de pertenencia ($\in$) y continencia ($\subseteq$) de conjuntos, estableciendo el método de doble inclusión para demostrar la igualdad entre conjuntos. Además, estudiaremos el conjunto vacío ($\varnothing$) y el conjunto potencia para cualquier conjunto A ($\mathcal{P}(A)$), y analizaremos la Paradoja de Russell. Después introduciremos las operaciones básicas entre conjuntos (unión, intersección, diferencia y complemento) y estableceremos propiedades importantes como la distributividad y las Leyes de De Morgan. También introduciremos el álgebra de conjuntos, método poderoso para demostrar igualdades entre conjuntos sin utilizar doble inclusión. Después estudiaremos otras operaciones entre conjuntos: la unión e intersección generalizada, las cuales están íntimamente ligadas a los cuantificadores lógicos, y el producto cartesiano, el cual servirá como base para el estudio de las relaciones y funciones en el capítulo 4.

Capítulo 2: Inducción: los números naturales

Estudiaremos la estructura ordenada de los números naturales ($\mathbb{N}$), estableciendo el llamado Principio del Buen Orden. Demostraremos que este principio es equivalente al Principio de Inducción Matemática, el cual nos servirá como método de demostración para muchas afirmaciones matemáticas asociadas a los números naturales. Después introduciremos la noción de isomorfismo entre estructuras ordenadas, la cual será retomada en el capítulo 6 desde una perspectiva más general. Finalmente, utilizando los métodos previamente establecidos de inducción y recursión, estudiaremos varios ejemplos de *conteo* —área de las matemáticas encargada de determinar cuántos objetos matemáticos poseen cierta propiedad— y calcularemos el tamaño de ciertos conjuntos finitos que son recurrentes en las matemáticas como, por ejemplo, el conjunto de todos los subconjuntos de un conjunto que tienen un tamaño dado.

Capítulo 3: Divisibilidad: los números enteros

Estudiaremos la relación de divisibilidad sobre los números enteros ($\mathbb{Z}$) —conjunto que será construido de forma rigurosa en el capítulo 4—, la cual nos permitirá definir las nociones de residuo, máximo común divisor, primos relativos y números primos. Estableceremos el Teorema Fundamental de la Aritmética, el cual permite descomponer de forma única a cada número natural positivo en factores primos. Después estudiaremos las congruencias módulo n y definiremos una estructura

llamada los "enteros módulo n" ($\mathbb{Z}_n$), la cual ejemplifica los conceptos de relación de equivalencia y grupo, que serán estudiados en detalle en los capítulos 4 y 6, respectivamente. Además, demostraremos dos teoremas clásicos de divisibilidad: el Pequeño Teorema de Fermat y el Teorema Chino del Residuo, el cual garantiza la solución de sistemas de congruencias lineales que cumplen con ciertas propiedades.

Capítulo 4: Relaciones y funciones

Introduciremos el concepto de relación como conjunto de pares ordenados y definiremos las nociones de dominio, imagen, inversa y composición. Estudiaremos la clausura reflexiva, simétrica y transitiva de una relación, en términos de las operaciones de unión e intersección generalizada estudiadas en el capítulo 1. Después nos enfocaremos en la noción de función como un caso especial de relación, definiendo además los conceptos de inyectividad, sobreyectividad y biyectividad; esta última será el pilar fundamental en la definición de que dos conjuntos tengan el mismo tamaño, la cual será estudiada en detalle en el capítulo 5. Después estudiaremos las relaciones de equivalencia, los conceptos de partición de un conjunto y de conjunto de representantes. Las relaciones de equivalencia permitirán la construcción de la estructura de los números enteros a partir de los números naturales, y la estructura de los números racionales ($\mathbb{Q}$) a partir de los números enteros, todo lo cual permite responder a ciertas preguntas cotidianas de conteo.

Capítulo 5: Cardinales

Definiremos la relación de equipotencia entre conjuntos, la cual formaliza la idea de que dos conjuntos tengan el mismo tamaño o cardinal. Demostraremos que ésta es una relación de equivalencia, lo cual nos permitirá clasificar los conjuntos. Primero definiremos los conjuntos finitos, demostrando que esta definición coincide con aquélla dada en el capítulo 2, y estableceremos sus propiedades mediante inducción matemática. Después estudiaremos los conjuntos enumerables, esto es, aquellos que son equipotentes con $\mathbb{N}$. Demostraremos que $\mathbb{Z}$ y $\mathbb{Q}$ son conjuntos enumerables. Finalmente estudiaremos los conjuntos infinitos no enumerables, cuyo infinito es mayor que aquél de $\mathbb{N}$. Demostraremos que el conjunto $\mathcal{P}(\mathbb{N})$ y el conjunto de los números reales ($\mathbb{R}$) son ambos infinitos no enumerables y equipotentes entre sí. También demostraremos que no existe un infinito mayor que todos los demás.

Capítulo 6: Estructuras matemáticas

Finalmente, daremos un panorama global, aunque simplificado, de las estructuras matemáticas, muchas de las cuales van más allá del alcance de este libro y a partir de las cuales se desarrollan las distintas ramas de las matemáticas (álgebra, análisis, combinatoria, probabilidad, teoría de números, geometría, etc). A partir de las nociones de conjunto, función y relación que establecimos en los capítulos anteriores, definiremos las estructuras relacionales, las algebras de Boole, los espacios métricos, los espacios topológicos y los grupos; estos últimos los estudiaremos en cierto detalle, enunciando sus propiedades principales y dando varios ejemplos. Finalmente estudiaremos los isomorfismos entre estructuras matemáticas, los cuales son biyecciones que "respetan la estructura"; por medio de ellos podemos capturar las propiedades esenciales de una estructura, "quitándonos las gafas" por así decirlo, esto es, olvidando los nombres de sus elementos.

Sobre los ejercicios

Durante la lectura de cada capítulo el lector se encontrará ocasionalmente con el siguiente mensaje:

☞ Antes de seguir leyendo

Es este caso le sugerimos que se detenga en la lectura e intente resolver los pequeños ejercicios que aparecen propuestos allí, con el fin de aclarar los conceptos que se han presentado. Adicionalmente, al final de cada sección se encuentra una serie de ejercicios. Recomendamos al lector intentar resolverlos durante un rato largo y, si no los puede resolver, seguir intentándolo. Es frecuente que el primer enfoque para resolver un ejercicio no sea el correcto, así que se deben hacer varios intentos y para ello ciertamente se requiere de persistencia.

Al final de cada capítulo el lector encontrará un proyecto, el cual consiste en una serie de ejercicios relacionados entre sí, cuyo estudio apunta a lograr una comprensión más profunda de algunos de los temas y conceptos ahí tratados. Se espera que con cada proyecto el lector pueda motivarse fuertemente a profundizar en su tema favorito, desarrollando así desde temprano el gusto por áreas particulares en las matemáticas tales como la combinatoria, la teorías axiomáticas, la teoría de grupos, la teoría de conjuntos y las matemáticas discretas.

AGRADECIMIENTOS

El autor está profundamente agradecido con Nicolás Vaughan, principal editor del libro, cuyo compromiso, profesionalismo, retroalimentación constante y trabajo serio han hecho posible su publicación con la mayor calidad posible. Además, agradece calurosamente a Aquiles Páramo, quien contribuyó enormemente en muchos aspectos del proyecto, aportando observaciones y sugerencias pertinentes, originales y exquisitas.

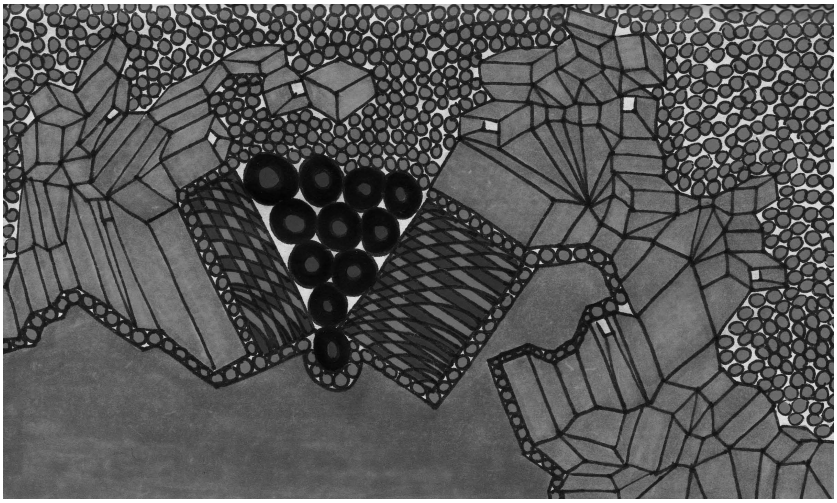
El autor quiere darle un reconocimiento especial a Ramiro de La Vega, principal revisor de contenido matemático, quien contribuyó de forma totalmente desinteresada con el libro, dándole equilibrio, estructura y rigor; mi sincero agradecimiento a Ramiro. Igualmente agradece enormemente a Andrea Solano por las maravillosas ilustraciones artísticas que acompañan el libro, las cuales esperamos que sirvan como inspiración matemática al lector. Asimismo, a David Laverde y Nicolás Vaughan por el diseño de las imágenes técnicas. El autor además agradece a Alejandro Forero, Sergio Tello, Alexander Berenstein, Felipe Castañeda, Luis Jaime Corredor, Carlos Montenegro, Xavier Caicedo, María Trujillo, Silvia Barbina, Maricarmen Martínez, Andrés "Betún" Betancourt, Federico Arboleda, Camilo Rengifo y Óscar Velásquez, por colaborar en diversos aspectos de este proyecto.

Finalmente, el autor agradece de forma sincera al Departamento de Matemáticas de la Universidad de los Andes, y en especial a su director, René Meziat, por el enorme apoyo prestado, en todo sentido posible, para la realización de este libro. Este libro no es otra cosa que fruto de los esfuerzos continuos de varios matemáticos del departamento durante décadas por enseñar las matemáticas de una manera rigurosa, estructurada, abarcadora y, sobre todo, creativa.

—Andrés Forero Cuervo, septiembre de 2009.

CAPÍTULO 1

CONJUNTOS



Todo es un conjunto...

La noción de conjunto, cuya teoría fue desarrollada a finales del siglo XIX por Georg Cantor, es posiblemente la noción más importante utilizada en las matemáticas modernas. Muchos objetos y conceptos matemáticos (relaciones, funciones, operaciones, grupos, anillos, grafos, espacios vectoriales, geometrías, topologías, los números naturales, etc.) se definen de forma precisa en términos conjuntistas. Por ejemplo, un grupo es un conjunto junto con una operación sobre él que tiene ciertas propiedades. Una topología es un conjunto de conjuntos, llamados "abiertos", que cumplen con varias condiciones. Puesto que la noción que permite construir objetos matemáticos complejos es la de conjunto, la pregunta fundamental parece ser la siguiente: ¿qué es un conjunto exactamente?

No nos molestamos por responder lo anterior, ya que esto da pie a un juego de nunca acabar. Pues, si un objeto es una colección, entonces ¿qué es una colección? Si una colección es una clase, entonces ¿qué es una clase? En vez de buscar definir un conjunto, vamos a establecer ciertos principios fundamentales que hablen sobre ellos y que permitan

manipularlos de manera efectiva. En vez de decir explícitamente qué son los conjuntos, los describiremos de forma general estableciendo sus propiedades fundamentales y desarrollando así su teoría.

§ 1.1 Conceptos fundamentales

Conjunto

En términos informales un conjunto es una colección de objetos. La noción básica para estudiar los conjuntos es la de *pertenencia*. Por ejemplo, sea H el conjunto de todos los seres humanos y d la persona Diego Reyes. Es claro que d es un miembro o elemento del conjunto H. Decimos entonces que *d pertenece a H* o que *d es un elemento de H* y escribimos:

$\in$: Pertenencia

$$d \in H.$$

Por el contrario, como el número $c = 3$ no es un ser humano, decimos que *c no pertenece a H* y escribimos:

$$c \notin H.$$

Todo esto es muy sencillo. Sin embargo, para entender la naturaleza y propiedades de los conjuntos, es conveniente hacer las siguientes observaciones:

(a) Conocer un conjunto equivale a conocer sus elementos. De esta forma, si A y B son conjuntos que tienen exactamente los mismos elementos, entonces son el mismo conjunto y escribimos $A = B$. Esto se lee: "A es igual a B".

(b) La notación de corchetes es una forma común de describir conjuntos. Por ejemplo, si A es el conjunto cuyos elementos son 3 y 5, y ninguno otro, podemos escribir:

$$A = \{3, 5\}.$$

(c) El orden en que listamos los elementos de un conjunto no es importante. Por ejemplo, $\{3, 5\} = \{5, 3\}$. En otras palabras, un conjunto se asemeja a una bolsa de dulces distintos que podemos revolver o "desordenar" sin que cambie. Al hacerlo, no perdemos la información sobre qué dulces pertenecen a la bolsa, es decir, qué elementos pertenecen al conjunto.

(d) Si un objeto pertenece a un conjunto, pertenece *exactamente* una vez a él. Por ejemplo, el conjunto $\{6, 6\}$ tiene exactamente un elemento: el número 6. Así, $\{6, 6\} = \{6\}$ pues ambos conjuntos tienen exactamente los mismos elementos, a saber, 6. Análogamente tenemos que $\{2, 3, 3, 2, 3\} = \{2, 3\}$.

(e) Un conjunto puede ser finito o infinito, según tenga un número finito o infinito de elementos. Por ejemplo, el conjunto $\{1, 3, 5, 7\}$

es finito pues tiene cuatro elementos. En cambio, el conjunto de los números impares positivos $\{1,3,5,7,\dots\}$ es infinito, pues nunca acabaríamos de escribir a todos sus elementos.

(f) Un conjunto puede carecer de elementos y cuando tiene esta propiedad se denomina un conjunto *vacío*. Más adelante demostraremos que en realidad existe un único conjunto vacío.

(g) Si c es una propiedad y x es un objeto, entonces se abreviará la afirmación "x tiene la propiedad c" así: $c(x)$. Por ejemplo, si $c(x)$ es la propiedad "x es un caballo", denotamos el conjunto de los x que tienen la propiedad c, "el conjunto de los caballos", como

$$\{x : c(x)\},$$

y lo leemos así: *el conjunto de los x tales que $c(x)$* (el conjunto de los x tales que x es un caballo).

(h) La notación de corchetes es conveniente para describir algunos conjuntos, pero hay que ser cuidadosos en su uso. Por ejemplo, podría pensarse que el conjunto $\{x,y\}$ es necesariamente un conjunto con dos elementos. Sin embargo, si $x = y$, se tiene entonces que $\{x,y\} = \{x\} = \{y\}$, y en tal caso sería un conjunto con un único elemento.

Ejemplo 1.1. Los siguientes son ejemplos de conjuntos:

(a) Sea A el conjunto cuyos únicos elementos son 2 y 7. Esto es, $2 \in A$, $7 \in A$ y para cualquier objeto x, si x es distinto de 2 y de 7, entonces $x \notin A$. El conjunto A se puede escribir como $A = \{2,7\}$. Gracias a las observaciones anteriores tenemos que

$$A = \{2,7\} = \{7,2\} = \{2,7,2,2\} = \{7,7,2,2\}, \text{ etc.}$$

(b) Si d es un objeto cualquiera, el conjunto que resulta de introducir a d en un conjunto y no introducir ningún otro objeto es $\{d\}$, el conjunto cuyo único elemento es d. El conjunto $\{d\}$ es llamado el *singleton* $\{d\}$.[1] Por ejemplo, si $A = \{1,2,3\}$, entonces $\{A\} = \{\{1,2,3\}\}$ es un *singleton*. Claramente A es distinto de $\{A\}$ ya que A tiene tres elementos, mientras que $\{A\}$ tiene tan sólo un elemento.

Singleton

[1] Aunque en la literatura matemática lo habitual es encontrar el anglicismo "*singleton*" —costumbre que aquí seguiremos—, en español también se lo suele llamar "conjunto unitario" o "uniconjunto".

ℕ: Números naturales

(c) Simbolizamos mediante $\mathbb{N}$ al conjunto de los números naturales, el cual se define como

$$\mathbb{N} := \{0, 1, 2, \dots\}.$$

$\mathbb{N}$ es un conjunto infinito y además tiene la siguiente notable propiedad: para todo n, si $n \in \mathbb{N}$, entonces $n + 1 \in \mathbb{N}$.

(d) Sea S el conjunto de todos los números naturales entre 4 y 900, incluyendo extremos. En lugar de listar todos los elementos de S, es conveniente escribir este conjunto como $\{x \in \mathbb{N} : 4 \leq x \leq 900\}$. Esto se lee: *el conjunto de los x en* $\mathbb{N}$ *tales que x es mayor o igual a* 4, *y menor o igual a* 900.

(e) Sea $D = \{3, 8, 13, 18, 23\}$. Entonces $D = \{3 + 5j : j = 0, 1, 2, 3, 4\}$, que se puede leer así: *D es el conjunto de los números de la forma* $3 + 5j$, *en donde j varía entre 0 y 4* . Por ejemplo, 13 es de la forma $3 + 5j$ (si se toma $j = 2$). Una manera alternativa de describir a D es la siguiente: sea $C = \{0, 1, 2, 3, 4\}$. Entonces $D = \{3 + 5j : j \in C\}$.

Notación extensional

Notación intensional

Los ejemplos (a), (b) y (c) ilustran maneras *extensionales* de nombrar conjuntos, en las cuales listamos sus elementos explícitamente; el ejemplo (d) describe otra forma de nombrarlos, *intensionalmente*, exhibiendo la propiedad común que comparten sus elementos; el ejemplo (e) muestra un conjunto representado de ambas maneras.

Toda forma extensional finita puede traducirse a una forma intensional: si

$$S = \{a_0, a_1, \dots, a_n\},$$

entonces podemos decir que $S = \{x : p(x)\}$, donde $p(x)$ es la propiedad "$x = a_0$ o $x = a_1$ o … o $x = a_n$". Sin embargo, muchas descripciones intensionales no tienen contraparte extensional (¿puede el lector pensar en ejemplos de ello?).

☞ **Antes de seguir leyendo**

1. ¿Cuántos elementos tiene el conjunto $\{1, \{6, 9\}\}$?
2. Liste todos los elementos del siguiente conjunto:
$$\{y : \text{ existe } k \in \mathbb{N} \text{ tal que } 0 < k < 5 \text{ y } y = 3 + 2k\}.$$
3. Sean $A = \{1, 2, 3, 4\}$ y $B = \{3, 4, 5, 6\}$. Sea C el siguiente conjunto:
$$C = \{x \in \mathbb{N} : \text{ si } x \in A \text{ entonces } x \in B\}.$$
Liste todos los elementos de C.

Subconjuntos

Sea H_{1843} el conjunto de los seres humanos que nacieron en el año 1843. Es claro que todo elemento de H_{1843} es también un elemento de $H = \{x : x \text{ es un ser humano}\}$, esto es: para todo x, si x pertenece a H_{1843}, entonces x pertenece a H. Lo anterior lo expresamos diciendo que H_{1843} es un *subconjunto* de H. Si simbolizamos "para todo" mediante el símbolo $\forall$, e "implica" mediante el símbolo $\to$, podemos formular la definición general de subconjunto de la siguiente manera:

$\forall$: *Para todo*

$\to$: *Implicación*

Definición 1.2. Sean A y B conjuntos. Diremos que A es un *subconjunto* de B (en símbolos, $A \subseteq B$) si

$\subseteq$: *Subconjunto*

$$\forall x : x \in A \to x \in B,$$

lo que se lee: "para todo x, si $x \in A$ entonces $x \in B$".

Por definición, las expresiones "$A \subseteq B$", "A es un subconjunto de B", "A está contenido en B" y "A está incluido en B" significan lo mismo. Sin embargo, éstas no significan lo mismo que la expresión "A pertenece a B". En otras palabras, las nociones de pertenencia y contenencia *son distintas* y no son intercambiables. Por ejemplo, un ser humano *no* está contenido en el conjunto H de los seres humanos, sino que *pertenece* a este conjunto. Por otra parte, el conjunto de los nigerianos no pertenece al conjunto de los africanos, sino que *está contenido* en él, ya que para todo x, si x es nigeriano, entonces x es africano.

En matemáticas es frecuente demostrar afirmaciones de la forma $A \subseteq B$. Esto significa demostrar que para todo x, si $x \in A$, entonces $x \in B$. La primera afirmación, $x \in A$, se llama la *hipótesis* (afirmación que suponemos verdadera) y la segunda afirmación, $x \in B$, se llama la *conclusión* (afirmación que debemos concluir a partir de la hipótesis). Esquemáticamente, una demostración de la afirmación $A \subseteq B$ tiene la forma siguiente:

Hipótesis

Conclusión

$$\text{Sea } x \in A\text{: entonces... entonces } x \in B.$$

Los puntos suspensivos en el esquema anterior representan distintas afirmaciones que se pueden concluir lógicamente a partir de la hipótesis de que $x \in A$. El objetivo es "llegar" a la afirmación $x \in B$. Este método de demostración se denomina *método de demostración por elementos*. Veamos un ejemplo:

Demostración por elementos

Ejemplo 1.3. Sean $A = \{12n : n \in \mathbb{N}\}$, $B = \{3k : k \in \mathbb{N}\}$. Demuestre que $A \subseteq B$.

Solución. Queremos demostrar que para todo x, si $x \in A$ entonces $x \in B$. Por ello comenzamos escribiendo: sea x tal que $x \in A$, entonces por definición de A, existe $n \in \mathbb{N}$ tal que $x = 12n$. Queremos demostrar que $x \in B$, es decir, que existe $k \in \mathbb{N}$ tal que $x = 3k$. Ahora, $x = 12n = 3(4n)$. Sea $k = 4n$. Entonces $x = 3k$ y claramente $k \in \mathbb{N}$, pues el producto de dos números naturales es un número natural. Luego, por definición del conjunto B, $3k \in B$. Como $x = 3k$, concluimos, como queríamos, que $x \in B$. ■

Ejemplo 1.4. Sean $A = \{n^3 : n \in \mathbb{N}, n > 1\}$, $B = \{k : k \in \mathbb{N}, k > 5\}$. Demuestre que $A \subseteq B$.

Solución. Queremos demostrar que para todo x, si $x \in A$ entonces $x \in B$. Por ello comenzamos escribiendo: sea $x \in A$. Entonces existe $n \in \mathbb{N}$ tal que $n > 1$ y $x = n^3$. Como $n > 1$ y n es un número natural, tenemos que $n \geq 2$. Entonces $x = n^3 \geq 2^3 = 8$. Claramente $x \in \mathbb{N}$ y $x > 5$, luego $x \in B$. ■

En general, en matemáticas para demostrar una afirmación de la forma "para todo x, si $p(x)$ entonces $q(x)$", se comenzará la demostración escribiendo "sea x tal que $p(x)$". En particular, para demostrar que $A \subseteq B$, es decir, que para todo x, si $x \in A$ entonces $x \in B$, la demostración deberá comenzar con "sea x tal que $x \in A$" o simplemente "sea $x \in A$".

☞ **Antes de seguir leyendo**

Sean $A = \{6n + 9 : n \in \mathbb{N}\}$, $B = \{3k : k \in \mathbb{N}\}$. Demuestre que $A \subseteq B$.

Observación 1.5. $A \supseteq B$ significa naturalmente $B \subseteq A$, lo que se puede leer *A es un superconjunto de B*.

Supongamos que $A \subseteq B$ y sea x cualquier objeto. Si x no pertenece a B, entonces x tampoco pertenecerá a A, ya que si x perteneciera a A, también pertenecería a B, lo cual contradice nuestra hipótesis de que $x \notin B$. En resumen:

$$\text{Si } A \subseteq B \text{ y } x \notin B, \text{ entonces } x \notin A.$$

La relación *no ser subconjunto* la denotamos con el símbolo $\not\subseteq$. Por ejemplo, si $A = \{1, 3, 5\}$ y $B = \{1, 7\}$, entonces A no es un subconjunto de B ya

que —por ejemplo— $3 \in A$ y $3 \notin B$. La afirmación $A \not\subseteq B$ es equivalente a la siguiente afirmación: "Existe x tal que $x \in A$ y $x \notin B$".

Igualdad de conjuntos

Sean A y B conjuntos,[2] y supongamos que $A \subseteq B$ y $B \subseteq A$. Esto quiere decir que A y B *tienen los mismos elementos*: todo x que pertenezca a A debe pertenecer a B y viceversa. Pues bien, en este caso lo más natural es que podamos concluir que A y B son en realidad el mismo conjunto. En otras palabras, la única razón para afirmar que dos conjuntos son distintos es que difieran en sus elementos. Dicha propiedad la expresamos en el siguiente principio:[3]

Principio 1.6 (Extensionalidad). Si los conjuntos A y B tienen exactamente los mismos elementos, entonces $A = B$.

PE: *Principio de Extensionalidad*

Si A y B son conjuntos y $A = B$, entonces claramente A y B tienen los mismos elementos. Ahora bien, gracias al Principio de Extensionalidad (PE), si A y B tienen los mismos elementos, entonces $A = B$. En resumen, las afirmaciones "$A = B$" y "A y B tienen los mismos elementos" son *equivalentes*, esto es, siempre que alguna de ellas sea verdadera, la otra también lo es.[4] De forma más concisa, escribimos:

Afirmaciones equivalentes

$$A = B \leftrightarrow A \text{ y } B \text{ tienen los mismos elementos,}$$

donde el símbolo $\leftrightarrow$ se lee "si y sólo si", y representa la equivalencia entre dos afirmaciones.

$\leftrightarrow$: *Equivalencia*

Observación 1.7 (Formas equivalentes para expresar la igualdad de conjuntos). Si A y B son conjuntos, las siguientes afirmaciones son equivalentes entre sí; esto es, siempre que alguna de ellas sea verdadera, entonces las demás también lo serán:

(a) $A = B$;

(b) A y B tienen los mismos elementos;

(c) $A \subseteq B$ y $B \subseteq A$;

(d) $(\forall x : x \in A \to x \in B)$ y $(\forall x : x \in B \to x \in A)$;

[2] En principio, podría ocurrir que $A = B$, pues dos nombres o símbolos distintos no garantizan que los objetos nombrados por ellos sean objetos distintos.

[3] Un principio es una afirmación que suponemos verdadera, pero no demostramos.

[4] Sobre la noción de equivalencia, véase el Apéndice A, Definición A.3 p. 299, abajo.

(e) $\forall x : x \in A \leftrightarrow x \in B$;

(f) para todo elemento x, o bien $x \in A$ y $x \in B$, o bien $x \notin A$ y $x \notin B$.

Observación 1.8. Una analogía útil con el PE es la siguiente: si a y b son números tales que $a \leq b$ y $b \leq a$, entonces $a = b$.

Demostración por doble inclusión

Por el PE, para demostrar que los conjuntos A y B son iguales, basta demostrar dos afirmaciones por separado: $A \subseteq B$ y $B \subseteq A$. A este método de demostración de igualdad de conjuntos lo denominaremos *demostración por doble inclusión*.

Para los dos ejemplos siguientes es necesario introducir el conjunto de los *números enteros*, definido como $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. Note que $\mathbb{N} \subseteq \mathbb{Z}$.

Ejemplo 1.9. Sea $A = \{y + 1 : y \in \mathbb{Z}\}$, $B = \{z + 3 : z \in \mathbb{Z}\}$. Demuestre mediante doble inclusión que $A = B$.

Solución. Demostraremos por separado que $A \subseteq B$ y $B \subseteq A$:

($\subseteq$) Queremos demostrar que para todo x, si $x \in A$, entonces $x \in B$. Comenzamos escribiendo: "sea x tal que $x \in A$". Ahora, como $x \in A$, entonces existe $y \in \mathbb{Z}$ tal que $x = y + 1$. Queremos ver que $x \in B$, esto es, que existe $z \in \mathbb{Z}$ tal que $x = z + 3$. Dado que $x = y + 1$, entonces

$$x = y + 1 = (y - 2) + 3.$$

Tomemos $z = y - 2$. Dado que $y \in \mathbb{Z}$, entonces $z \in \mathbb{Z}$. Además $x = z + 3$. Hemos demostrado que existe $z \in \mathbb{Z}$ tal que $x = z + 3$, luego $x \in B$, como queríamos.

($\supseteq$) Queremos demostrar que para todo x, si $x \in B$ entonces $x \in A$. Comenzamos escribiendo: "sea x tal que $x \in B$". Ahora, como $x \in B$ entonces existe $z \in \mathbb{Z}$ tal que $x = z + 3$. Queremos ver que $x \in A$, esto es, que existe $y \in \mathbb{Z}$ tal que $x = y + 1$. Dado que $x = z + 3$, entonces

$$x = z + 3 = (z - 2) + 1.$$

Tomemos $y = z - 2$. Dado que $z \in \mathbb{Z}$, entonces $y \in \mathbb{Z}$. Además $x = y + 1$. Hemos demostrado que existe $y \in \mathbb{Z}$ tal que $x = y + 1$; luego $x \in A$, como queríamos. ■

Ejemplo 1.10. Sea $A = \{4y+1 : y \in \mathbb{Z}\}$, $B = \{9-4z : z \in \mathbb{Z}\}$. Demuestre mediante doble inclusión que $A = B$.

Solución. Demostraremos por separado que $A \subseteq B$ y $B \subseteq A$:

(⊆) Sea $x \in A$. Entonces existe $y \in \mathbb{Z}$ tal que $x = 4y+1$. Queremos ver que $x \in B$, esto es, que existe $z \in \mathbb{Z}$ tal que $x = 9-4z$. Dado que $x = 4y+1$, entonces

$$x = 4y+1 = 9-9+4y+1 = 9-8+4y = 9-4(2-y).$$

Tomemos $z = 2-y$. Dado que $y \in \mathbb{Z}$, entonces $z \in \mathbb{Z}$. Además $x = 9-4z$. Hemos demostrado que existe $z \in \mathbb{Z}$ tal que $x = 9-4z$; luego $x \in B$, como queríamos.

(⊇) Sea $x \in B$. Entonces existe $z \in \mathbb{Z}$ tal que $x = 9-4z$. Queremos ver que $x \in A$, esto es, que existe $y \in \mathbb{Z}$ tal que $x = 4y+1$. Dado que $x = 9-4z$, entonces:

$$x = 9-4z = 8-4z+1 = 4(2-z)+1.$$

Tomemos $y = 2-z$. Dado que $z \in \mathbb{Z}$, entonces $y \in \mathbb{Z}$. Además $x = 4y+1$. Hemos demostrado que existe $y \in \mathbb{Z}$ tal que $x = 4y+1$; luego $x \in A$, como queríamos. ∎

A veces la relación de ser subconjunto es *estricta*, en el sentido de que no se da una igualdad:

Definición 1.11. Sean A y B conjuntos. Diremos que A es *subconjunto propio*[5] de B (y lo notamos como $A \subset B$ o $A \subsetneq B$) si $A \subseteq B$ y $A \neq B$.

⊂ ó ⊊: Subconjunto propio

Por ejemplo, $\{1,2\} \subset \{1,2,3,4\}$ y $\{\} \subset \{2,3\}$. Como el lector puede verificar, la afirmación $A \subset B$ es equivalente a: $A \subseteq B$ y existe x tal que $x \in B$ y $x \notin A$.

☞ **Antes de seguir leyendo**

1. ¿Verdadero o falso? Dados dos conjuntos A y B, siempre vale por lo menos alguna de las siguientes afirmaciones: $A \subseteq B$ o $B \subseteq A$. ¿Cómo se compagina esto con la analogía de los números propuesta anteriormente?
2. Calcule el número de subconjuntos propios de $\{1,2\}$.

[5] Debe advertirse que en algunos libros de matemáticas el símbolo $\subset$ es utilizado para referirse a la relación $\subseteq$ de contenencia.

El conjunto vacío

Sea V un conjunto. Decimos que V es un conjunto *vacío*, y lo simbolizamos como $\varnothing$, si no tiene ningún elemento. Dicho de otro modo, el conjunto V es vacío si $\forall x : x \notin V$.

∃: *Existe*

Naturalmente, un conjunto es *no vacío* si existe algún elemento x que le pertenece. Si representamos la palabra "existe" con el símbolo $\exists$, tenemos que un conjunto V es no vacío si y sólo si

$$\exists x : x \in V,$$

lo que se lee: "existe x tal que x pertenece a V".

Es fácil pensar en conjuntos no vacíos: pensar en $\{2, 3\}$ es pensar en el 2 y el 3, y pensar en $\mathbb{N}$ es pensar en infinitos números: $0, 1, 2, \ldots$ En contraste, pensar en un conjunto vacío equivale a pensar en nada. A continuación establecemos, como principio, que existe por lo menos un conjunto con la propiedad de ser vacío:

Principio 1.12 (Principio del conjunto vacío). Existe un conjunto V que es vacío, esto es, que cumple la siguiente propiedad:

$$\forall x : x \notin V.$$

¿Existen múltiples conjuntos vacíos diferentes entre sí? La respuesta es que no. A continuación damos una demostración de este hecho.

Teorema 1.13. Si V y V' son conjuntos vacíos, entonces $V = V'$.

Prueba. Sean V y V' conjuntos vacíos. Entonces por definición, tenemos que

$$\forall x : x \notin V \text{ y } \forall x : x \notin V'.$$

Demostraremos que $V \subseteq V'$ y que $V' \subseteq V$. Supongamos que $V \nsubseteq V'$. Esto significa, por la definición de $\nsubseteq$, que existe x tal que $x \in V$ y $x \notin V'$. Sin embargo, la existencia de un x tal que $x \in V$ contradice la hipótesis de que V es conjunto vacío, de modo que en realidad no puede ocurrir que $V \nsubseteq V'$; por lo tanto, $V \subseteq V'$. De manera análoga podemos demostrar que $V' \subseteq V$. Como $V \subseteq V'$ y $V' \subseteq V$, concluimos por el PE que $V = V'$. ∎

Este teorema nos autoriza a utilizar un símbolo para referirnos al conjunto vacío, ya que éste es único. Este símbolo será $\varnothing$, o también $\{\}$. Si abreviamos "existe un único" por $\exists!$, lo que hemos mostrado es lo siguiente: $\exists! Y : \forall x : x \notin Y$. Por definición, el conjunto vacío es un conjunto finito (pues tiene 0 elementos).

∅: *Vacío*

☞ **Antes de seguir leyendo**

1. Demuestre que $\forall A : \varnothing \subseteq A$. En otras palabras, que todo conjunto contiene al conjunto vacío.
2. ¿Es todo objeto del universo un conjunto? ¿Por qué? (*Ayuda*: la definición de un conjunto *no* puede ser "algo que tiene elementos"; si lo fuera, $\varnothing$ no sería un conjunto, lo cual estaría en contradicción con el Principio 1.12.)

Supongamos que queremos encontrar una propiedad que sólo la tenga el número 2. Por ejemplo, la propiedad $p(x) :=$ "*x es par*" es una propiedad relativa a 2, pero otros números también la tienen. En cambio, la propiedad $q(x) :=$ "x es un número primo par" es una propiedad que sólo el 2 cumple, como se verá en el capítulo 3. Decimos, entonces que la propiedad *q caracteriza* al número 2.

La propiedad de *ser un conjunto vacío*, definida anteriormente, al ser satisfecha por un único objeto, lo caracteriza y le da su nombre: "el conjunto vacío". Veamos una caracterización alternativa del conjunto vacío, esto es, otra propiedad que lo distingue del resto de los conjuntos. Esta propiedad es la de *ser subconjunto de todos los conjuntos*.

Teorema 1.14. Para todo conjunto A tenemos que $A = \varnothing \leftrightarrow (\forall B : A \subseteq B)$.

Prueba. Sea A un conjunto. Una proposición de la forma $p \leftrightarrow q$ es equivalente a $(p \to q)$ y $(q \to p)$. Por ende, para demostrar la afirmación

$$A = \varnothing \leftrightarrow (\forall B : A \subseteq B),$$

debemos demostrar por separado las dos siguientes:

$$\text{(a)}\ \ A = \varnothing \to (\forall B : A \subseteq B); \qquad \text{(b)}\ \ (\forall B : A \subseteq B) \to A = \varnothing.$$

La parte (a) se simboliza como $(\to)$ y la parte (b) como $(\leftarrow)$:

$(\to)$ Supongamos que $A = \varnothing$. Sea B un conjunto. Debemos demostrar que $A \subseteq B$. Por la definición de subconjunto, debemos demostrar que, para todo x,

$$x \in A \to x \in B.$$

Sea x dado; como la afirmación "$x \in A$" es falsa (ya que $A = \varnothing$), podemos aplicar la Ley del Antecedente Falso (véase el Apéndice A) para concluir que la afirmación "$x \in A \to x \in B$" es verdadera. Concluimos que $A \subseteq B$, como queríamos.

(←) Supongamos que $\forall B : A \subseteq B$. Debemos concluir que $A = \varnothing$. Según la hipótesis, A es un subconjunto de todo conjunto B. En particular, si tomamos $B = \varnothing$, concluimos que

$$A \subseteq \varnothing.$$

Por otra parte, por lo recién demostrado en (→), sabemos que el conjunto vacío tiene la propiedad de ser un subconjunto de todos los conjuntos y, en particular, de A. Entonces

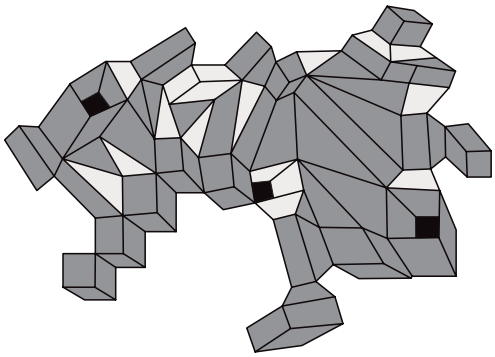
$$\varnothing \subseteq A.$$

Por el PE podemos entonces concluir que $A = \varnothing$, lo que queríamos demostrar. ∎

Doble implicación

Las demostraciones con el formato anterior son llamadas *demostraciones por doble implicación*. Éstas son bastante comunes en matemáticas y tienen la ventaja de que permiten partir una demostración en dos demostraciones más sencillas.

Ejercicios



1. Calcule los siguientes conjuntos haciendo una lista de todos sus elementos:
   (a) $A = \{2x + 1 : x \in \mathbb{N} \text{ y } x < 5\}$;
   (b) $A = \{y : \text{ existe } a \in \mathbb{N} \text{ tal que } 1 \leq a \leq 5 \text{ y } y = 2a\}$;
   (c) $A = \{x \in \mathbb{N} : x < 4 \text{ o } 100 < x^2 < 150\}$;
   (d) $A = \{-(x - 10) : x \in \{1, 2, 3\}\}$;
   (e) $A = \{x \in \mathbb{N} : x < 0\}$;
   (f) $A = \{x : x \subseteq \{1\}\}$.

2. Sea x un número natural. Determine, si es posible, el número exacto de elementos en cada uno de los siguientes conjuntos:
   (a) $\{3\}$,
   (b) $\{2,2,2\}$,
   (c) $\{1,3,1,-3\}$,
   (d) $\{\}$,
   (e) $\{x\}$,
   (f) $\{1,\{2,3,4\}\}$,
   (g) $\{2,\{3,4\},\{4,2\}\}$,
   (h) $\{2,\{3,4\},\{4,2\},\{4,3\}\}$,
   (i) $\{n \in \mathbb{N} : n^2 < 16\}$,
   (j) $\{n \in \mathbb{N} : n > 6\}$,
   (k) $\{x,-x,x^2\}$,
   (l) $\{x,x+1\}$.
3. Sean $A = \{1,2,3,4,5\}$, $B = \{2,4,6,8,10\}$ y $C = \{x : x \in A \leftrightarrow x \notin B\}$. Liste explícitamente todos los elementos de C.
4. Sean $A = \{x :$ existe $k \in \mathbb{N}$ tal que $x = 6k\}$ y $B = \{x :$ existe $a \in \mathbb{N}$ tal que $x = 2a$ y existe $b \in \mathbb{N}$ tal que $x = 3b\}$. Demuestre mediante el método de elementos que $A \subseteq B$. ¿Es verdad que $A = B$?
5. Sea $A = \{y :$ existe $n \in \mathbb{N}$ tal que $4 < n < 8$ y $y = 2n+1\}$. Otra forma de describirlo es: $A = \{2n+1 : n \in \mathbb{N}, 4 < n < 8\}$. Describa el conjunto A *extensionalmente*.
6. Sea $A = \{1,2,\ldots,n\}$ (donde $n \in \mathbb{N}^*$).[6] Calcule el número de subconjuntos de A que tienen:
   (a) 0 elementos,
   (b) 1 elemento,
   (c) $n-1$ elementos,
   (d) n elementos.
7. Recuerde que $\mathbb{Z} = \{\ldots,-2,1,0,1,2,\ldots\}$ es el conjunto de los números enteros. Sea A el conjunto $A = \{3s+1 : s \in \mathbb{Z}\}$.
   (a) Demuestre que $-11 \in A$. (*Ayuda*: demuestre que existe un número entero s tal que $-11 = 3s+1$.)
   (b) Demuestre que $8 \notin A$.
   (c) ¿Qué conjunto es $B = \{x \in \mathbb{Z} : x \notin A\}$?
8. Demuestre por el método de doble inclusión las siguientes igualdades de conjuntos:
   (a) $\{3x+1 : x \in \mathbb{Z}\} = \{1-3y : y \in \mathbb{Z}\}$;
   (b) $\{\pi(n-2) : n \in \mathbb{Z}\} = \{\pi(n+10) : n \in \mathbb{Z}\}$;
   (c) $\{2x+5 : x \in \mathbb{Z}\} = \{1+2y : y \in \mathbb{Z}\}$;
   (d) $\{x+1 : x \in \mathbb{N}, x < 7\} = \{w : w \in \mathbb{N}, 0 < w < 8\}$;
   (e) $\{-(x+2) : x \in \mathbb{N}\} = \{y \in \mathbb{Z} : y \leq -2\}$.

[6] Por definición, $\mathbb{N}^*$ es el conjunto de los números naturales, sin incluir el 0; esto es, $\mathbb{N}^* := \{1,2,3,\ldots\}$.

9. Los ejercicios siguientes relacionan la lógica proposicional con la igualdad de conjuntos. Recuerde que una propiedad $c(x)$, al ser aplicada a un determinado valor $x \in \mathbb{N}$, será verdadera o falsa.

   (a) Sean $p(x)$, $d(x)$ y $e(x)$ propiedades relativas a números naturales y sean A y B los siguientes conjuntos:

   $$A = \{x \in \mathbb{N} : \text{ si } p(x) \text{ entonces } d(x) \text{ y } q(x)\};$$
   $$B = \{x \in \mathbb{N} : \text{ si } p(x) \text{ entonces } q(x)\}.$$

   Demuestre que $A \subseteq B$.

   (b) Sean $p(x)$ y $q(x)$ propiedades relativas a números naturales, y sean A y B los siguientes conjuntos:

   $$A = \{x \in \mathbb{N} : p(x) \text{ es falsa}\};$$
   $$B = \{x \in \mathbb{N} : \text{ si } p(x) \text{ entonces } q(x)\}.$$

   Demuestre que $A \subseteq B$.

   (c) Sean $q(x)$ y $r(x)$ propiedades relativas a números naturales. Sea $s(x)$ la propiedad $[q(x) \text{ y } r(x)]$ y sean A y B los siguientes conjuntos:

   $$A = \{x \in \mathbb{N} : \text{ es falso que } s(x)\};$$
   $$B = \{x \in \mathbb{N} : \text{ si } q(x), \text{ entonces } r(x) \text{ es falsa}\}.$$

   Demuestre que $A = B$.

   (d) Sean $q(x)$ y $r(x)$ propiedades relativas a números naturales. Sea $s(x)$ la propiedad $(q(x) \text{ o } r(x))$ y sean A y B los siguientes conjuntos:

   $$A = \{x \in \mathbb{N} : \text{ es falso que } s(x)\};$$
   $$B = \{x \in \mathbb{N} : q(x) \text{ es falsa y } r(x) \text{ es falsa}\}.$$

   Demuestre que $A = B$.

   (e) Sean $p(x)$ y $q(x)$ propiedades relativas a números naturales y sean A, B y C los siguientes conjuntos:

   $$A = \{x \in \mathbb{N} : \text{ si } p(x) \text{ entonces } q(x)\};$$
   $$B = \{x \in \mathbb{N} : x \notin A\};$$
   $$C = \{x \in \mathbb{N} : p(x) \text{ es verdadera y } q(x) \text{ no es verdadera}\}.$$

   Demuestre que $B = C$.

10. Los ejercicios siguientes consisten en encontrar propiedades precisas que permitan describir la pertenencia a ciertos conjuntos.

    (a) Sea X el conjunto $\{6, 10, 14, 18, 22, \dots\}$. Describa a X intensionalmente, es decir, encuentre una propiedad $p(x)$, tal que X sea igual a $\{x \in \mathbb{N} : p(x)\}$. (*Ayuda*: véase el ejercicio 5.)

(b) Sea $2\mathbb{N}$ el conjunto de los números naturales pares, esto es, $2\mathbb{N} := \{0, 2, 4, \dots\}$. Describa al conjunto $2\mathbb{N}$ *intensionalmente*; más precisamente, encuentre una propiedad $p(x)$ tal que $2\mathbb{N} = \{x \in \mathbb{N} : p(x)\}$. (*Ayuda*: un número par es un número de la forma $2k$, donde k es un número entero.)

(c) Sea X el conjunto de los números primos. Un número primo es un número natural mayor que 1, cuyo único divisor mayor que 1 es él mismo. Describa a X intensionalmente (hay varias formas de hacerlo).

11. Sea $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$. Calcule el siguiente conjunto haciendo una lista de todos sus elementos: $C = \{\{x, y\} : x \in A, y \in B\}$.

12. Dados los conjuntos A y B, diremos que A es un *vecino inferior de* B si A es un subconjunto propio de B y no existe un conjunto X tal que A es un subconjunto propio de X y X un subconjunto propio de B. Con base en tal definición, resuelva los siguientes ejercicios:

(a) Sea $B = \{0, 1, \dots, n\}$. Calcule el número de vecinos inferiores de dicho conjunto.

(b) Si B es un conjunto que tiene un número infinito de vecinos inferiores A, ¿es necesariamente B un conjunto infinito? Justifique su respuesta.

(c) Demuestre que A es un vecino inferior de B si y sólo si se cumple lo siguiente: A es subconjunto de B y existe x tal que x no pertenece a A, y todo elemento de B que sea distinto de x pertenece a A.

(d) Demuestre que si B es un conjunto infinito, entonces B tiene un número infinito de vecinos inferiores.

§ 1.2 Propiedades de la relación ⊆ y el conjunto potencia

Consideremos el conjunto de los números naturales:

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\},$$

ordenado por la relación $\leq$. Como ejemplos de esta relación tenemos que $4 \leq 10$, $10 \leq 17$, $4 \leq 17$ y $17 \leq 17$. La relación $\leq$ cumple con tres propiedades fundamentales:

(a) *reflexividad*: $\forall x : x \leq x$ (todo número natural es menor o igual a sí mismo);

(b) *antisimetría*: $\forall x, y : (x \leq y \text{ y } y \leq x) \to x = y$ (dados los números naturales x y y, si x es menor o igual a y y viceversa, entonces $x = y$);

(c) *transitividad*: $\forall x, y, z : (x \leq y \text{ y } y \leq z) \to x \leq z$ (dados los números naturales x, y y z, si x es menor o igual a y, y y es menor o igual a z, entonces x es menor o igual a z).

Las anteriores tres propiedades también son válidas en el contexto de los conjuntos, con respecto a la relación $\subseteq$:

Teorema 1.15. Dados los conjuntos A, B y C, se cumplen las siguientes propiedades:

(a) *reflexividad*: $\forall A : A \subseteq A$;

(b) *antisimetría*: $\forall A, B : (A \subseteq B \text{ y } B \subseteq A) \to A = B$;

(c) *transitividad*: $\forall A, B, C : (A \subseteq B \text{ y } B \subseteq C) \to A \subseteq C$.

Prueba.

(a) Es evidente, puesto que para todo x, si $x \in A$, entonces $x \in A$.

(b) Esto es válido en virtud del PE.

(c) Debemos demostrar que $A \subseteq C$, suponiendo como hipótesis que $A \subseteq B$ y $B \subseteq C$. Sea $x \in A$. Como $A \subseteq B$, entonces $x \in B$. Como $B \subseteq C$, entonces $x \in C$. ∎

Orden parcial

Una relación que cumpla con las tres propiedades del teorema anterior se denomina un *orden parcial*. Tanto $\leq$ como $\subseteq$ son órdenes parciales (el primero ordena a los números, el segundo a los conjuntos). Las reflexiones anteriores sugieren cierto parecido estructural entre el universo de los números naturales con su relación de orden y el universo de los subconjuntos de $\mathbb{N}$ con la relación de contenencia o inclusión. Además de que ambos universos se encuentran parcialmente ordenados, en ambos encontramos un mínimo: el 0 es menor o igual a cualquier número natural y el conjunto vacío está contenido en cualquier conjunto. En este sentido, el número 0 y el conjunto vacío cumplen con el mismo papel, pero en contextos distintos.

Dados los conjuntos A y B, entonces sucede exactamente una de las siguientes cuatro posibilidades (véase la Figura 1.1):

(a) $A \subseteq B$ pero $B \nsubseteq A$; en este caso puede verse que $A \subset B$ (A es un subconjunto propio de B);

(b) $B \subseteq A$ pero $A \nsubseteq B$ (es decir, $B \subset A$);

(c) $A \subseteq B$ y $B \subseteq A$: en este caso, $A = B$;

(d) $A \nsubseteq B$ y $B \nsubseteq A$: en este caso decimos que los conjuntos A y B no son *comparables* entre sí. *Comparabilidad*

En la Figura 1.1 utilizamos los llamados *diagramas de Venn*, los cuales representan conjuntos de manera informal, en donde cada uno se representa mediante una región típicamente circular. Estos diagramas sirven para ilustrar propiedades de contenencia o no contenencia entre conjuntos. *Diagramas de Venn*

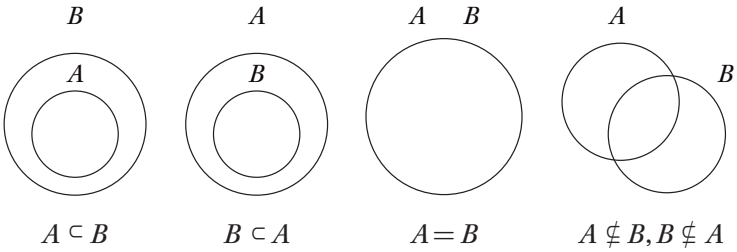


Figura 1.1 : Dados los conjuntos A y B, ocurre una y sólo una de estas cuatro posibilidades.

Un ejemplo en el cual sucede la situación (d) es el siguiente: tomemos los conjuntos $A = \{1, 2, 3\}$ y $B = \{2, 3, 4, 5\}$. En este caso $A \nsubseteq B$ (ya que $1 \in A$ y $1 \notin B$) y $B \nsubseteq A$ (ya que $5 \in B$ y $5 \notin A$).

Un *orden total* es una relación de orden en la cual todos los elementos son comparables entre sí; es decir, dados dos elementos, alguno de ellos es menor que el otro, o los elementos son iguales. Como hemos notado, el orden parcial ⊆ en los conjuntos *no* es un orden total. Por el contrario, el orden ≤ sobre $\mathbb{N}$ permite comparar a todo par de números naturales. Este orden parcial *es* un orden total. *Orden total*

La totalidad (también llamada *linealidad*) del orden ≤ sobre $\mathbb{N}$, permite imaginar a sus elementos como ordenados en una fila infinita, con mínimo y sin máximo. Por su parte, la no totalidad del orden ⊆ en los conjuntos sólo permite visualizarlos como un árbol, con varias ramas bifurcantes, pero sin un "orden absoluto", por así decirlo.

Una analogía útil respecto de esta cuestión es la siguiente. Algunas personas creen que existe una lista que ordena todas las películas existentes así: la mejor, la segunda mejor, etc. Para estas personas, todas las películas son comparables, es decir, dadas dos películas A y B, o A es mejor que B, o B es mejor que A, o A y B son la misma película. Estas personas creen que el orden *ser mejor que* de las películas es un orden total, similar al orden ≤ sobre $\mathbb{N}$. Alternativamente, algunas personas son incapaces de comparar ciertas películas, argumentando que "la primera tiene aspectos que la segunda no tiene, pero la segunda tiene otros que

la primera no tiene", etc. Sin embargo, en algunos casos sí consideran que cierta película es mejor que otra. Estas personas creen que el orden *ser mejor que* de las películas es un orden parcial, pero no total, similar al orden de los conjuntos.

> ☞ **Antes de seguir leyendo**
>
> 1. Demuestre que si A está contenido en B y C no está contenido en B, entonces C no está contenido en A.
> 2. Determine si son comparables los conjuntos $A = \{n \in \mathbb{N} : n > 5\}$ y $B = \{n \in \mathbb{N} : n^2 > 36\}$, es decir, si alguno de ellos es un subconjunto del otro.

Conjunto potencia

Sea A un conjunto. Evidentemente el conjunto de todos los elementos de A es A mismo: $A = \{x : x \in A\}$. Sin embargo, el conjunto de todos sus subconjuntos resulta ser bien distinto y en general más complejo.

$\mathcal{P}(A)$: Conjunto potencia

Definición 1.16 (Conjunto potencia). Dado un conjunto A, definimos el conjunto *potencia de A* (o *partes de A*) como:

$$\mathcal{P}(A) := \{B : B \subseteq A\}.$$

Esto es, para todo conjunto B, $B \in \mathcal{P}(A) \leftrightarrow B \subseteq A$.

> **Ejemplo 1.17**. Algunos ejemplos del conjunto potencia:
>
> (a) Sea $A_1 = \{1\}$. Entonces $\mathcal{P}(A_1) = \{\varnothing, \{1\}\}$, un conjunto con dos elementos. Note que aunque $\{1\} \in \mathcal{P}(A_1)$, $\{1\} \notin A_1$.
>
> (b) Sea $A_2 = \{1, 2\}$. Entonces
>
> $$\mathcal{P}(A_2) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\},$$
>
> un conjunto con 4 elementos.
>
> (c) Sea $A_3 = \{1, 2, 3\}$. Entonces
>
> $$\mathcal{P}(A_3) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\},$$
>
> un conjunto con 8 elementos (véase la Figura 1.2.)
>
> (d) $\mathcal{P}(\varnothing) = \{\varnothing\}$. Para ver esto, basta preguntarse qué conjunto S es candidato a ser subconjunto de $\varnothing$: si S tiene al menos un

elemento x, entonces $x \notin \varnothing$ y, por ende, $S \nsubseteq \varnothing$; y esto quiere decir que $S \notin \mathcal{P}(\varnothing)$. Ahora, como $\varnothing \subseteq \varnothing$, entonces por definición $\varnothing \in \mathcal{P}(\varnothing)$.

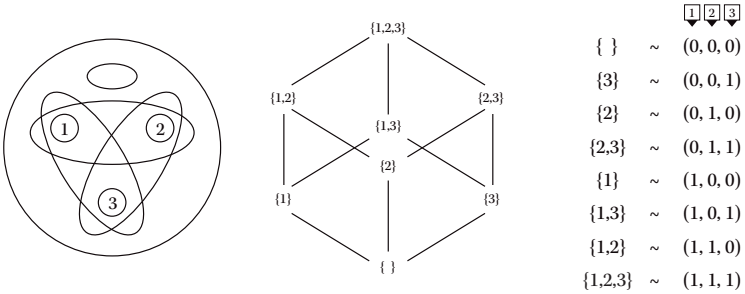


Figura 1.2: Distintas representaciones del conjunto $\mathcal{P}(\{1,2,3\})$.

En la Figura 1.2 podemos ver tres representaciones del conjunto $\mathcal{P}(\{1,2,3\})$. La primera consiste en un diagrama de Venn, en donde representamos visualmente los conjuntos por regiones del plano. En la segunda se construye el "retículo" en el cual se dibujan líneas siempre que haya contenencia (sin pintar todas las líneas posibles). En la tercera se asocia a cada conjunto $S \in \mathcal{P}(\{1,2,3\})$ una sucesión de ceros y unos, $f_S = (f_0, f_1, f_2)$, en donde $f_i = 1$ si $i \in S$ y $f_i = 0$ si $i \notin S$. Por ejemplo, al conjunto $S = \{1,3\}$ se le asocia la sucesión $f_S = (1,0,1)$, puesto que $1 \in S$, $2 \notin S$ y $3 \in S$.

Teorema 1.18. Sean A y B conjuntos. Tenemos:

(a) $\varnothing \in \mathcal{P}(A)$ y $A \in \mathcal{P}(A)$;
(b) $\mathcal{P}(A) \neq \varnothing$;
(c) $A \subseteq B \leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$;
(d) $A = B \leftrightarrow \mathcal{P}(A) = \mathcal{P}(B)$.

Prueba.

(a) Como $\varnothing \subseteq A$, entonces, por definición, $\varnothing \in \mathcal{P}(A)$. Como $A \subseteq A$, entonces, también por definición, $A \in \mathcal{P}(A)$.

(b) Es una consecuencia inmediata de (a).

(c) Utilizamos el método de doble implicación:

($\rightarrow$) Supongamos que $A \subseteq B$ y demostremos que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Sea $S \in \mathcal{P}(A)$. Entonces $S \subseteq A$. Como $A \subseteq B$, por transitividad de la relación $\subseteq$ concluimos que $S \subseteq B$, es decir, $S \in \mathcal{P}(B)$.

(←) Supongamos que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Por (a) se tiene que $A \in \mathcal{P}(A)$. Entonces $A \in \mathcal{P}(B)$, lo cual implica que $A \subseteq B$.

(d) Utilizamos el método de doble implicación:

(→) Supongamos que $A = B$. Entonces $A \subseteq B$ y $B \subseteq A$; si aplicamos (c) en ambas contenencias, concluimos que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ y $\mathcal{P}(B) \subseteq \mathcal{P}(A)$. Por el PE concluimos que $\mathcal{P}(A) = \mathcal{P}(B)$.

(←) Se razona de manera análoga. ■

La Paradoja de Russell

Es natural suponer que a partir de cualquier propiedad podemos construir el conjunto de los objetos que cumplen con ella. Sin embargo, este no es el caso, como se muestra a continuación.

Sea $p(x)$ la propiedad "$x \notin x$". Entonces $A = \{x : p(x)\} = \{x : x \notin x\}$ es el conjunto de los conjuntos que no pertenecen a sí mismos. ¿Pertenece A a A? Hay dos posibles respuestas a esta pregunta:

> (i) Supongamos que $A \in A$: por definición de A, $p(A)$ es verdadera, luego $A \notin A$, contradiciendo la suposición original.

> (ii) Supongamos entonces que $A \notin A$: por definición de la propiedad p, vale $p(A)$ y, por definición del conjunto A, tenemos que $A \in A$, lo que de nuevo contradice la hipótesis.

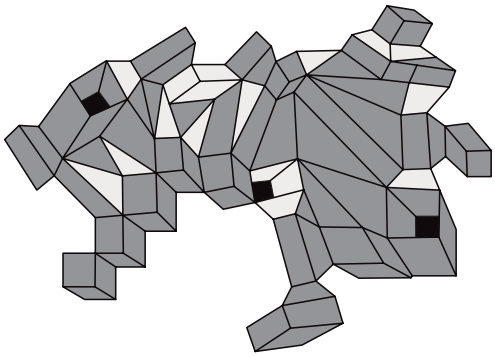
En cualquier caso llegamos a una contradicción. Concluimos que el conjunto A anteriormente descrito no existe. Esta paradoja se conoce con el nombre de *Paradoja de Russell*. La moraleja de esta paradoja es que no podemos darle existencia a un conjunto únicamente a partir de una propiedad que imaginemos. Sin embargo, existe el llamado *Axioma de Separación*, que permite hacerlo en algunos casos (véase el ejercicio 11).

Paradoja de Russell

☞ **Antes de seguir leyendo**

1. Roberto es un pintor de un pueblo que pinta a aquellas personas que no se pintan a sí mismas. ¿Se pinta Roberto a sí mismo?
2. Supongamos que a Salomé le gusta conducir, pero no le gusta bailar. Ana dice: "A Salomé le gusta bailar, le gusta conducir, y lo que ella dice sobre mí es verdadero". Salomé, por otra parte, afirma: "De las tres cosas que Ana dice sobre mí, dos o más son falsas". ¿Es la afirmación de Salomé verdadera o falsa? ¿Es la última afirmación de Ana verdadera o falsa?

Ejercicios



1. Sea $x = \{1, 2, 3, 4\}$.
   (a) Liste todos los elementos de $\mathcal{P}(x)$. ¿Cuántos son?
   (b) Sea $y = x \cup \{5\}$. Liste todos los elementos de $\mathcal{P}(y)$ que *no* son elementos de $\mathcal{P}(x)$.
2. Sea $A = \{1, 3\}$.
   (a) Calcule el conjunto $\mathcal{P}(A)$. ¿Cuántos elementos tiene?
   (b) Calcule el conjunto $\mathcal{P}(\mathcal{P}(A))$. ¿Cuántos elementos tiene?
   (c) ¿Cuántos elementos tiene el conjunto $\mathcal{P}(\mathcal{P}(\mathcal{P}(A)))$?
3. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:

   (a) $\forall x : x \supset \varnothing$;
   (b) $\forall x : \varnothing \in x$;
   (c) $\varnothing \in \varnothing$;
   (d) $\varnothing \in \{\{\}\}$;
   (e) $\varnothing \subseteq \{\{\}\}$;
   (f) $\varnothing = \{\varnothing\}$;
   (g) $\{\varnothing, x\} \subseteq \mathcal{P}(x)$;
   (h) $\{5\} \in \mathbb{N}$;
   (i) $\{5\} \subseteq \mathbb{N}$;
   (j) $\{1, \{5\}\} \subseteq \mathbb{N}$;
   (k) $\{x : x \neq x\} = \varnothing$;
   (l) $\forall x : \mathcal{P}(x) \neq \varnothing$.

4. Dé un ejemplo de conjuntos A, B, C, D y E tales que A no sea vacío, A pertenezca a B, B sea un subconjunto propio de C, C pertenezca a D y D sea un subconjunto propio de E. Responda las siguientes preguntas de acuerdo con su ejemplo (justifique claramente su respuesta):

(a) ¿Pertenece A a C?
(b) ¿Es A subconjunto de C?
(c) ¿Pertenece B a D?
(d) ¿Es B un subconjunto de E?
(e) ¿Es D un subconjunto de E?

5. Sean $A = \{1, 2\}$, $B = \{2, 3\}$. Liste todos los x tales que x es subconjunto de A o x es un subconjunto de B.
6. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:
   (a) para todo conjunto A, $A \subseteq \mathcal{P}(\mathcal{P}(A))$;
   (b) para todo conjunto A, $\mathcal{P}(A) \in \mathcal{P}(\mathcal{P}(A))$.
7. Considere la relación $\subset$ de contenencia propia entre conjuntos. ¿Es $\subset$ una relación reflexiva? ¿Es $\subset$ una relación antisimétrica? ¿Es $\subset$ una relación transitiva?
8. Demuestre que si A tiene n elementos (donde n es un número natural), entonces $\mathcal{P}(A)$ tiene 2^n elementos. (*Ayuda*: suponga que $A = \{a_1, \ldots, a_n\}$. Represente a cada subconjunto de A como una n-tupla de ceros y unos, como se ejemplificó en la Figura 1.2.)
9. En este ejercicio definimos relaciones de "contenencia aproximada" entre conjuntos.
   (a) Sean A y B conjuntos, y $n \in \mathbb{N}$. Diremos que $A \subseteq_n B$ si y sólo si el conjunto $\{x \in A : x \notin B\}$ es un conjunto a lo sumo con n elementos, esto es, tiene menos de $n + 1$ elementos. Demuestre que la relación $\subseteq_n$ es reflexiva, pero en general no es antisimétrica ni transitiva salvo en el caso $n = 0$.
   (b) Demuestre que si $n, m \in \mathbb{N}$ y $n \leq m$, entonces la relación $\subseteq_n$ es más *fuerte* que la relación $\subseteq_m$. En otras palabras, si $A \subseteq_n B$ entonces $A \subseteq_m B$.
   (c) Dados los conjuntos A y B, diremos que $A \subseteq_* B$ si y sólo si el conjunto $\{x \in A : x \notin B\}$ es un conjunto finito. Demuestre que la relación $\subseteq_*$ es reflexiva y transitiva, pero en general no es antisimétrica.
10. Dados los conjuntos A, B y C, diremos que A y B son *iguales módulo* C (en símbolos, $A =_C B$) si y sólo si se cumple lo siguiente:

    Para todo $x \in C$, $x \in A$ si y sólo si $x \in B$.

    Informalmente, $A =_C B$ si el conjunto C "no es capaz de detectar la posible diferencia entre los conjuntos A y B". Demuestre las siguientes afirmaciones:

(a) Si $A = B$, entonces $A =_C B$, y dé un ejemplo en el cual $A =_C B$, pero $A \neq B$.

(b) Si $A_1 =_C A_2$ y $A_2 =_C A_3$, entonces $A_1 =_C A_3$.

(c) Si $A_1 =_C A_2$ y $B \subseteq C$, entonces $A_1 =_B A_2$.

(d) $A =_A B$ si y sólo si $A \subseteq B$.

11. El Axioma de Separación afirma (aproximadamente) lo siguiente: dado un conjunto A y una propiedad $p(x)$, existe un conjunto B tal que $\forall x : x \in B \leftrightarrow (x \in A \text{ y } p(x))$. En otras palabras, B es el conjunto de los elementos de A con la propiedad p.

    (a) Demuestre que el conjunto B descrito arriba es único, es decir, que si existe B' tal que $\forall x : x \in B' \leftrightarrow (x \in A \text{ y } p(x))$, entonces necesariamente $B' = B$.

    (b) Utilice el Axioma de Separación y la Paradoja de Russell para demostrar que no existe el "conjunto de todos los conjuntos": esto es, que no existe un conjunto A tal que para todo x, $x \in A$.

12. Este ejercicio está relacionado con la Paradoja de Russell. Dada una palabra cualquiera, diremos que es *autológica* si ella se aplica a sí misma, y *heterológica* si ella no se aplica a sí misma. Por ejemplo, las palabras "esdrújula" y "larguisisisísima" son autológicas, mientras que las palabras "persona" y "rara" son heterológicas.

    (a) La palabra "autológica" ¿es autológica o heterológica?

    (b) La palabra "heterológica" ¿es autológica o heterológica?

§ 1.3 Operaciones básicas entre conjuntos

En esta sección definiremos las operaciones básicas entre conjuntos, a saber, unión, intersección, diferencia y complemento; dichas operaciones nos permiten construir nuevos conjuntos a partir de otros.

Unión e intersección

Si P y Q son dos afirmaciones, entonces la afirmación "P o Q" será verdadera si por lo menos alguna de las afirmaciones P y Q es verdadera. Por ejemplo, la afirmación "$x \in \{1, 2\}$ o $x \in \{2, 3\}$" será verdadera si $x = 1$, si $x = 2$, si $x = 3$ y será falsa si $x = 4$. (Para más sobre el uso del término "o" (la disyunción), véase el Apéndice A, pp. 298 ss, abajo.)

∪: *Unión*

Definición 1.19 (Unión). Dados los conjuntos A y B, definimos el conjunto $A \cup B$ así:

$$A \cup B := \{x : x \in A \text{ o } x \in B\}.$$

El conjunto $A \cup B$ se denomina la *unión entre* A y B, A *unión* B, o también A *unido con* B (véase la Figura 1.3).

∨: *Disyunción*

Simbolizando el término "o" como $\vee$, entonces para todo x vale que

$$x \in A \cup B \leftrightarrow (x \in A \vee x \in B).$$

Ejemplo 1.20. Si $A = \{1, 2, 3, 4\}$ y $B = \{1, 3, 4, 5, 7\}$, entonces

$$A \cup B = \{1, 2, 3, 4, 5, 7\}.$$

Note que el conjunto $A \cup B$ incluye a todo elemento que pertenece por lo menos a alguno de los conjuntos A o B. De ahí que $6 \notin A \cup B$, ya que $6 \notin A$ y $6 \notin B$.

Tal como el ejemplo anterior lo ha ilustrado, en general vale la siguiente equivalencia:

$$(x \notin A \cup B) \leftrightarrow (x \notin A \text{ y } x \notin B).$$

∩: *Intersección*

Definición 1.21 (Intersección). Dados los conjuntos A y B, definimos el conjunto $A \cap B$ así:

$$A \cap B := \{x : x \in A \text{ y } x \in B\}.$$

El conjunto $A \cap B$ se denomina la *intersección entre* A *y* B, A *intersección* B o también A *intersecado con* B (véase la Figura 1.3).

∧: *Conjunción*

Simbolizando el término "y" como $\wedge$, entonces para todo x vale que

$$x \in A \cap B \leftrightarrow (x \in A \wedge x \in B).$$

Ejemplo 1.22. Si $A = \{1, 2, 3\}$ y $B = \{1, 3, 4, 5\}$, se tiene entonces que $A \cap B = \{1, 3\}$. Note que $A \cap B$ incluye únicamente los elementos que aparecen en ambos conjuntos A y B. Por ejemplo, $2 \in A$ pero $2 \notin B$, de modo que $2 \notin A \cap B$.

Si A y B son conjuntos, tenemos que para todo x, x no pertenece al conjunto $A \cap B$ si y sólo si x no se encuentra simultáneamente en A y B, esto es, si $x \notin A$ o $x \notin B$:

$$(x \notin A \cap B) \leftrightarrow (x \notin A \vee x \notin B).$$

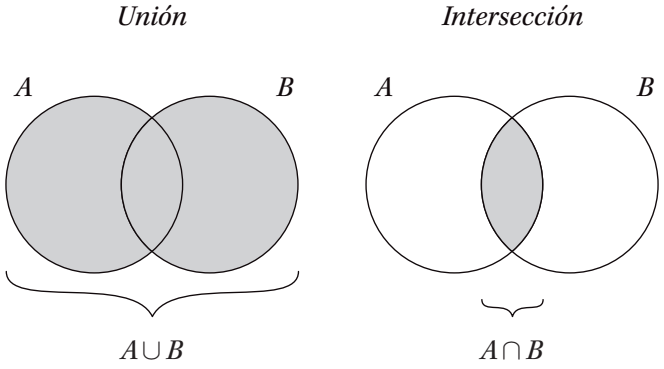


Figura 1.3: Unión e intersección de conjuntos. Intuitivamente la unión es un conjunto "grande", mientras que la intersección es un conjunto "pequeño".

Diremos que A y B son *disjuntos* (*entre sí*) si $A \cap B = \varnothing$. En otras palabras, A y B son disjuntos si no tienen elementos en común.

Conjuntos disjuntos

☞ **Antes de seguir leyendo**

Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso (dados los conjuntos A, B y C):

1. Si $A \cup B = A \cup C$, entonces $B = C$.
2. Si $A \cap B = A \cap C$, entonces $B = C$.
3. Si $A \cup B = A \cup C$ y $A \cap B = A \cap C = \varnothing$, entonces $B = C$.
4. A y $\varnothing$ son disjuntos.
5. Si A y B son disjuntos y B y C son disjuntos, entonces A y C son disjuntos.
6. Si A tiene 5 elementos y B tiene 6 elementos, entonces $A \cup B$ tiene 11 elementos.

Ahora tomamos un conjunto cualquiera $\mathcal{U}$ y trabajamos "dentro de $\mathcal{P}(\mathcal{U})$"; esto significa que todos los conjuntos que consideremos serán subconjuntos de $\mathcal{U}$. Llamaremos a $\mathcal{U}$ nuestro *universo de discurso*, o simplemente el *universo*.

$\mathcal{U}$: Universo

Las siguientes propiedades de la unión y la intersección son evidentes y se basan en las propiedades lógicas de los conectivos de disyunción y conjunción ($\vee$ y $\wedge$).

Teorema 1.23. Sean $A, B \subseteq \mathcal{U}$ conjuntos. Entonces se cumplen las siguientes propiedades:

(a) *idempotencia*: $A \cup A = A$, $A \cap A = A$;

(b) *conmutatividad*: $A \cup B = B \cup A$, $A \cap B = B \cap A$;

(c) *absorción*: $A \subseteq A \cup B$, $A \cap B \subseteq A$;

(d) *identidad*: $A \cup \varnothing = A$, $A \cap \mathcal{U} = A$;

(e) *piso y techo*: $A \cap \varnothing = \varnothing$, $A \cup \mathcal{U} = \mathcal{U}$;

(f) *asociatividad*: $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$.

Prueba.

(a) Demostremos que $A \cup A = A$. Para ello utilizamos el método de doble inclusión:

(⊆) Si $x \in A \cup A$, entonces $x \in A$ o $x \in A$. Pero entonces $x \in A$.

(⊇) Si $x \in A$, entonces $x \in A$ o $x \in A$, luego $x \in A \cup A$.

La demostración de que $A \cap A = A$ es análoga y se deja al lector (ejercicio 17).

(b) Demostremos que $A \cap B = B \cap A$. Para ello utilizamos el método de doble inclusión:

(⊆) Si $x \in A \cap B$, entonces $x \in A$ y $x \in B$. Pero entonces $x \in B$ y $x \in A$ y, por ende, $x \in B \cap A$.

(⊇) Si $x \in B \cap A$, entonces $x \in B$ y $x \in A$. Pero entonces $x \in A$ y $x \in B$ y, por ende, $x \in A \cap B$.

La demostración de que $A \cup B = B \cup A$ se deja al lector (ejercicio 17).

(c) Veamos que $A \subseteq A \cup B$: si $x \in A$, entonces es verdadero que $x \in A$ o $x \in B$,[7] luego $x \in A \cup B$. Ahora demostremos que $A \cap B \subseteq A$: si $x \in A \cap B$, entonces $x \in A$ y $x \in B$, y así $x \in A$. Esto demuestra que $A \cap B \subseteq A$.

(d) Demostremos que $A \cup \varnothing = A$. Para ello utilizamos el método de doble inclusión:

(⊆) Si $x \in A \cup \varnothing$, entonces $x \in A$ o $x \in \varnothing$. Pero la segunda opción es imposible, luego $x \in A$.

(⊇) Se tiene gracias a la propiedad (c).

La demostración de que $A \cap \mathcal{U} = A$ se deja al lector (ejercicio 17).

[7] Si p y q son proposiciones y p es verdadera, entonces la proposición (p o q) también lo será. En la demostración en cuestión, la afirmación ($x \in A$) juega el papel de p, y la afirmación ($x \in B$) el de q.

(e) Demostremos primero que $A \cup \mathcal{U} = \mathcal{U}$. Para ello utilizamos el método de doble inclusión:

(⊆) Si $x \in A \cup \mathcal{U}$, entonces $x \in A$ o $x \in \mathcal{U}$. Como $A \subseteq \mathcal{U}$, concluimos que en cualquier caso $x \in \mathcal{U}$.

(⊇) Se tiene gracias a las propiedades (b) y (c).

Veamos ahora que $A \cap \varnothing = \varnothing$: por (b) y (c) tenemos que $A \cap \varnothing \subseteq \varnothing$. Pero el único subconjunto de $\varnothing$ es $\varnothing$, luego $A \cap \varnothing = \varnothing$.

(f) Demostremos que $(A \cup B) \cup C = A \cup (B \cup C)$. Para ello utilizamos el método de doble inclusión:

(⊆) Si $x \in (A \cup B) \cup C$, entonces hay dos casos:

(i) $x \in A \cup B$: entonces $x \in A$ o $x \in B$. Pero ya que $B \subseteq B \cup C$ (por la propiedad (c)), entonces necesariamente $x \in A$ o $x \in B \cup C$, es decir, $x \in A \cup (B \cup C)$.

(ii) $x \in C$: entonces, por las propiedades (b) y (c), $x \in B \cup C$; y, si utilizamos de nuevo dichas propiedades, concluimos que $x \in A \cup (B \cup C)$.

En cualquier caso tenemos que $x \in A \cup (B \cup C)$, como queríamos demostrar.

(⊇) Es similar a la demostración de (⊆).

La demostración de que $(A \cap B) \cap C = A \cap (B \cap C)$ se deja al lector (ejercicio 17). ∎

Como el lector podrá notar, en el teorema anterior pudimos haber utilizado la propiedad (c) como instrumento para demostrar una de las dos contenencias en (a). Por otra parte, el método utilizado en la prueba de (f) se llama *demostración por casos*.[8]

Demostración por casos

Se examina cada uno de los casos que plantea una proposición que contiene disyunciones, y si todos conducen a la misma conclusión, entonces puede afirmarse esta conclusión. Otro teorema, menos evidente, caracteriza de dos maneras distintas la relación de contenencia:

Teorema 1.24. Dados dos conjuntos A y B, tenemos:

(a) $B \subseteq A$ si y sólo si $A \cup B = A$;

(b) $B \subseteq A$ si y sólo si $A \cap B = B$.

[8] Para más información sobre la demostración por casos, consúltese el Apéndice A, p. 304, abajo.

Prueba.

(a) Utilizamos el método de doble implicación:

(→) Supongamos que $B \subseteq A$. Debemos demostrar que $A \cup B = A$. Utilizamos el método de doble inclusión:

(⊆) Si $x \in A \cup B$, entonces $x \in A$ o $x \in B$: como todo elemento de B es elemento de A (por la hipótesis de que $B \subseteq A$), entonces en cualquier caso se tiene que $x \in A$.

(⊇) Si $x \in A$, entonces $x \in A \cup B$ por el Teorema 1.23 (c).

(←) Supongamos que $A \cup B = A$. Debemos demostrar que $B \subseteq A$. Sea $x \in B$. Entonces por el Teorema 1.23 (b) y (c), $x \in A \cup B$, pero por hipótesis este conjunto es igual a A, luego $x \in A$.

(b) Utilizamos el método de doble implicación:

(→) Supongamos que $B \subseteq A$. Debemos demostrar que $A \cap B = B$. Utilizamos el método de doble inclusión:

(⊆) Si $x \in A \cap B$, entonces $x \in B$ por el Teorema 1.23 (b) y (c).

(⊇) Si $x \in B$, entonces como $B \subseteq A$, $x \in A$. Entonces $x \in A \cap B$.

(←) Supongamos que $A \cap B = B$. Debemos probar que $B \subseteq A$. Sea $x \in B$. Entonces $x \in A \cap B$ (pues $A \cap B = B$), luego $x \in A$ por el Teorema 1.23 (c). ∎

La operación $\cup$ es una operación *binaria*. Por esto, una expresión de la forma $A \cup B \cup C$ en principio es ambigua y debe traducirse como $(A \cup B) \cup C$ o $A \cup (B \cup C)$. Pero en virtud del Teorema 1.23 (f) ambas expresiones denotan el mismo conjunto. Por lo tanto, definimos $A \cup B \cup C$ como $(A \cup B) \cup C$ (o $A \cup (B \cup C)$). Esta observación también vale si sustituimos uniformemente $\cup$ por $\cap$.

Ahora relacionamos las operaciones de unión e intersección entre sí mediante las llamadas *Leyes de Distribución*:

Leyes de Distribución

Teorema 1.25 (Distribución). Dados los conjuntos A, B y C, tenemos:

(a) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$;

(b) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Prueba.

(a) Utilizamos el método de doble inclusión:

(⊆) Sea $x \in (A \cup B) \cap C$. Entonces $x \in A \cup B$ y $x \in C$. Por lo primero, $x \in A$ o $x \in B$. Si $x \in A$, entonces $x \in A \cap C$. Si $x \in B$, entonces $x \in B \cap C$. Luego $x \in A \cap C$ o $x \in B \cap C$, es decir, $x \in (A \cap C) \cup (B \cap C)$.

(⊇) Sea $x \in (A \cap C) \cup (B \cap C)$. Entonces $x \in A \cap C$ o $x \in B \cap C$:

(i) $x \in A \cap C$: como $x \in A$, entonces $x \in A \cup B$, y como $x \in C$, tenemos que $x \in (A \cup B) \cap C$.

(ii) $x \in B \cap C$: como $x \in B$, entonces $x \in A \cup B$, y como $x \in C$, tenemos que $x \in (A \cup B) \cap C$.

En cualquier caso, $x \in (A \cup B) \cap C$.

(b) Se deja al lector (ejercicio 16). ∎

Teorema 1.26 (Absorción). Dados A y B conjuntos, tenemos:

(a) $A \cup (A \cap B) = A$; (b) $A \cap (A \cup B) = A$.

Prueba.

(a) Utilizamos el método de doble inclusión:

(⊆) Sea $x \in A \cup (A \cap B)$. Tenemos dos casos:

(i) $x \in A$: entonces $x \in A$.

(ii) $x \in A \cap B$: entonces $x \in A$ y $x \in B$, luego $x \in A$.

En cualquier caso concluimos que $x \in A$, como queríamos.

(⊇) Sea $x \in A$, entonces por el Teorema 1.23 (c), $x \in A \cup (A \cap B)$.

(b) Por el Teorema de distribución (Teorema 1.25), tenemos que

$$A \cap (A \cup B) = (A \cap A) \cup (A \cap B) = A \cup (A \cap B) = A.$$

La última igualdad es verdadera por la parte (a). ∎

En lo que resta de esta sección conviene que expliquemos el concepto de *contraejemplo*. Para ello consideremos la siguiente proposición: *Contraejemplo*

$$x^2 > x.$$

En ella, x representa el valor de un número natural cualquiera. Hay dos posibilidades respecto de esta afirmación:

(i) que la proposición sea verdadera para todos los valores de $x \in \mathbb{N}$; o bien,

(ii) que no se dé el anterior caso. Es decir, que la proposición sea falsa para *al menos* un valor de $x \in \mathbb{N}$.

De hecho, el segundo caso es el que se da, pues si tomamos, por ejemplo, $x = 1 \in \mathbb{N}$, entonces la afirmación $x^2 > x$ es falsa. Este ejemplo es llamado un *contraejemplo* para la proposición $(\forall x \in \mathbb{N} : x^2 > x)$, ya que contradice la verdad general de ella. A partir de este contraejemplo podemos concluir que la afirmación $(\forall x \in \mathbb{N} : x^2 > x)$ es falsa.

Ejemplo 1.27. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:

(a) Dados A y B, si $A \cup B = \varnothing$, entonces $A = \varnothing$ y $B = \varnothing$.

(b) Dados A y B, si $A \cap B = \varnothing$, entonces $A = \varnothing$ o $B = \varnothing$.

(c) Dados A y B, si $A \cap B \neq \varnothing$, entonces $A \neq \varnothing$ y $B \neq \varnothing$.

(d) Dados A y B, $(A \cap B) \cup B = A \cup B$.

Solución.

(a) Es verdadera. Veamos la demostración: si $A \cup B = \varnothing$, entonces como $A \subseteq A \cup B$ y $B \subseteq A \cup B$, concluimos que $A \subseteq \varnothing$ y $B \subseteq \varnothing$. Pero el único subconjunto de $\varnothing$ es $\varnothing$, luego $A = \varnothing$ y $B = \varnothing$.

(b) Es falsa. Veamos un contraejemplo: sea $A = \{1\}$, $B = \{2\}$. Se cumple que $A \cap B = \varnothing$, pero no se cumple que $A = \varnothing$ o $B = \varnothing$.

(c) Es verdadera. Veamos la demostración: si $A \cap B \neq \varnothing$, entonces existe x tal que $x \in A \cap B$. Entonces $x \in A$ y $x \in B$, y ello implica que $A \neq \varnothing$ y $B \neq \varnothing$.

(d) Es falsa. Veamos un contraejemplo: sea $A = \{1, 2\}$, $B = \{2, 3\}$. Entonces $(A \cap B) \cup B = \{2, 3\}$ mientras que $A \cup B = \{1, 2, 3\}$.

Diferencia y complemento

Así como podemos restar dos números, también podemos restar dos conjuntos de una manera natural. Esta operación se llama la *diferencia entre conjuntos* (véase la Figura 1.4).

$\setminus$: *Diferencia*

Definición 1.28 (Diferencia). Dados A y B conjuntos, definimos $A \setminus B$ como el conjunto

$$A \setminus B := \{x \in A : x \notin B\}.$$

Entonces tenemos que para todo x, $x \in A \setminus B \leftrightarrow (x \in A \wedge x \notin B)$. El conjunto $A \setminus B$ se denomina *A menos B*, o también *la diferencia entre A y B*.

Ejemplo 1.29. Algunos ejemplos de diferencia entre conjuntos:

(a) $\{1, 0, 2, -3, 3, 15, 4, -20\} \setminus \{1, -3, 15, 4\} = \{0, 2, 3, -20\}$;

(b) Si $A = \{0, 4, 7, 10\}$ y $B = \{3, 4, 8, 10, 12\}$, entonces $A \setminus B = \{0, 7\}$ y $B \setminus A = \{3, 8, 12\}$;

(c) $\{3, 5, 7\} \setminus \mathbb{N} = \varnothing$;

(d) $\mathbb{Z} \setminus \mathbb{N} = \{-1, -2, -3, \cdots\}$.

(e) $\{1, 2\} \setminus \{3, 4\} = \{1, 2\}$.

☞ **Antes de seguir leyendo**

Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso (para A y B conjuntos):

1. $A \subseteq A \setminus B$.
2. $(A \cup B) \setminus B = A$.
3. Si A y B son disjuntos, entonces $A \setminus B = A$.
4. $A \nsubseteq B$ si y sólo si $A \setminus B \neq \varnothing$. 5. $A \subset B$ si y sólo si $B \setminus A \neq \varnothing$.

Ahora definimos el *complemento* de un conjunto $A \subseteq \mathcal{U}$ con respecto al universo del discurso $\mathcal{U}$ (véase la Figura 1.4):

Definición 1.30 (Complemento). Para un conjunto $A \subseteq \mathcal{U}$, definimos su *complemento* A^c con respecto a $\mathcal{U}$ como la diferencia entre $\mathcal{U}$ y A,[9] esto es,

A^c: *Complemento*

$$A^c := \mathcal{U} \setminus A.$$

Note que $A^c \subseteq \mathcal{U}$, puesto que, por definición, afirmar que x pertenece a A^c equivale a decir que $x \in \mathcal{U}$ y x *no* pertenece a A. Si simbolizamos el "no" mediante $\neg$, tenemos que para cualquier x:

$\neg$: *Negación*

$$x \in A^c \leftrightarrow (x \in \mathcal{U} \wedge \neg(x \in A)).$$

[9] Algunos autores suelen simbolizar el complemento de A como $\bar{A}$, $\neg A$, A' o $\sim A$.

Ejemplo 1.31. En este ejemplo tomamos como universo al conjunto $\mathcal{U} = \mathbb{N} = \{0, 1, 2, \dots\}$. Esto significa que sólo consideramos subconjuntos de $\mathbb{N}$. Sean los conjuntos $A = \{1, 5, 6\}$, $B = \{3, 7, 8, 10\}$ y $C = \{n \in \mathbb{N} : n > 3\} = \{4, 5, 6, 7, \dots\}$. Entonces:

(a) $A^c = \{n \in \mathbb{N} : n \neq 1 \wedge n \neq 5 \wedge n \neq 6\} = \{0, 2, 3, 4, 7, 8, 9, 10, 11, \dots\}$;

(b) $(A \cup B)^c = \{0, 2, 4, 9, 11, 12, 13, \dots\}$;

(c) $C^c = \{n \in \mathbb{N} : n < 4\} = \{0, 1, 2, 3\}$.

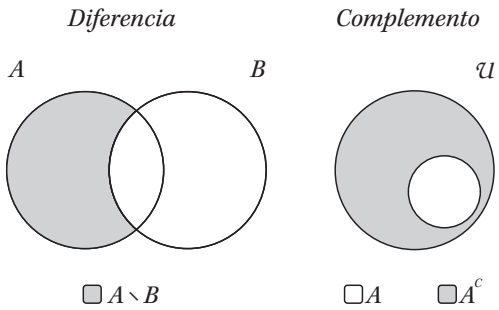


Figura 1.4: Diferencia y complemento de conjuntos. El complemento es un caso especial de la diferencia.

Dos propiedades notables del complemento son que para todo conjunto $A \subseteq \mathcal{U}$, A y su complemento son disjuntos, y además que $\mathcal{U}$ se puede escribir como la unión disjunta entre A y su complemento. Decimos "unión disjunta" para resaltar el hecho de que los conjuntos son disjuntos. Éste es el contenido del siguiente teorema:

Teorema 1.32 (Todo o nada). Para todo $A \subseteq \mathcal{U}$:[10]

$$\text{(a) } A \cap A^c = \varnothing; \qquad \text{(b) } A \cup A^c = \mathcal{U}.$$

Prueba. Sea A un conjunto. Demostraremos por separado que (a) y (b) son verdaderas:

Método de contradicción

(a) Queremos ver que $A \cap A^c = \varnothing$. Para ello utilizamos el método de contradicción,[11] el cual consiste en suponer que lo que queremos demostrar es falso, y a partir de esto llegar a una contradicción.

[10] Estas propiedades también son llamadas *leyes de complementariedad*.

[11] Para más información sobre este método, véase el Apéndice A, p. 302, abajo.

Supongamos que $A \cap A^c \neq \varnothing$. Entonces existe x tal que $x \in A \cap A^c$. De modo que $x \in A$ y $x \notin A$, lo cual es absurdo ya que un elemento no puede pertenecer y no pertenecer simultáneamente a un conjunto. Concluimos que $A \cap A^c = \varnothing$.

(b) Utilizamos el método de doble inclusión:

($\subseteq$) Sea $x \in A \cup A^c$. Dado que tanto A como A^c son subconjuntos de $\mathcal{U}$, entonces $x \in \mathcal{U}$.

($\supseteq$) Sea $x \in \mathcal{U}$. Si $x \in A$, entonces $x \in A \cup A^c$. Si por el contrario $x \notin A$, entonces por definición de complemento, $x \in A^c$, luego $x \in A \cup A^c$. En cualquier caso tenemos que $x \in A \cup A^c$. ∎

Veamos ahora otras propiedades menos evidentes del complemento:

Teorema 1.33. Para A, B subconjuntos de $\mathcal{U}$:

(a) $A \setminus B = A \cap B^c$;

(b) *doble complemento*: $(A^c)^c = A$;

(c) $A \subseteq B$ si y sólo si $B^c \subseteq A^c$.

Prueba.

(a) Para un x arbitrario, $x \in A \setminus B$ si y sólo si ($x \in A$ y $x \notin B$), y esto equivale a $x \in A \cap B^c$.

(b) Utilizamos el método de doble inclusión:

($\subseteq$) Si $x \in (A^c)^c$, entonces $x \in \mathcal{U} = A \cup A^c$ y $x \notin A^c$, luego necesariamente $x \in A$.

($\supseteq$) Si $x \in A$, entonces $x \in \mathcal{U}$. Pero además $x \notin A^c$, pues de lo contrario se tendría que $x \notin A$, entonces por definición de complemento, $x \in (A^c)^c$.

(c) Utilizamos el método de doble implicación:

($\rightarrow$) Supongamos que $A \subseteq B$. Debemos demostrar que $B^c \subseteq A^c$. Sea $x \in B^c$. Entonces $x \in \mathcal{U}$ y $x \notin B$. Este último hecho, junto con la hipótesis, implica que $x \notin A$ (pues de lo contrario x sería un elemento de B), así que $x \in A^c$.

($\leftarrow$) Supongamos que $B^c \subseteq A^c$. Por la implicación que acabamos de establecer, donde B^c sustituye a A y A^c sustituye a B, tenemos que $(A^c)^c \subseteq (B^c)^c$, y esto junto con (b) garantiza el resultado. ∎

La prueba de la propiedad (a) no fue descompuesta en dos inclusiones como de costumbre, sino que consistió en demostrar directamente que

pertenecer al primer conjunto equivale a pertenecer al segundo. Esta forma de demostración se llama el *método directo* para demostrar una igualdad de conjuntos. Pese a su elegancia, el lector se dará cuenta con la experiencia de que muchas pruebas de igualdad de conjuntos son más claras si se utiliza el método de doble inclusión.

Método directo

Leyes de De Morgan

Teorema 1.34 (Leyes de De Morgan). Para $A, B \subseteq \mathcal{U}$:

(a) $(A \cup B)^c = A^c \cap B^c$ (*el complemento de la unión es la intersección de los complementos*).

(b) $(A \cap B)^c = A^c \cup B^c$ (*el complemento de la intersección es la unión de los complementos*).

Prueba. Dejaremos la prueba de (a) al lector (ejercicio 1) y demostraremos (b). Utilizamos el método de doble inclusión:

($\subseteq$) Si $x \in (A \cap B)^c$, entonces $x \in \mathcal{U}$ y $x \notin A \cap B$; esto último implica que $x \notin A$ o $x \notin B$. Por ende, necesariamente $x \in A^c$ o $x \in B^c$, esto es, $x \in A^c \cup B^c$.

($\supseteq$) Si $x \in A^c \cup B^c$, entonces tenemos dos casos:

(i) $x \in A^c$: entonces $x \in \mathcal{U}$ y $x \notin A$, luego $x \notin A \cap B$. Por lo tanto, $x \in (A \cap B)^c$.

(ii) $x \in B^c$: si razonamos de forma análoga a como lo hicimos en (i), concluimos que $x \in (A \cap B)^c$.

En cualquier caso, $x \in (A \cap B)^c$. ∎

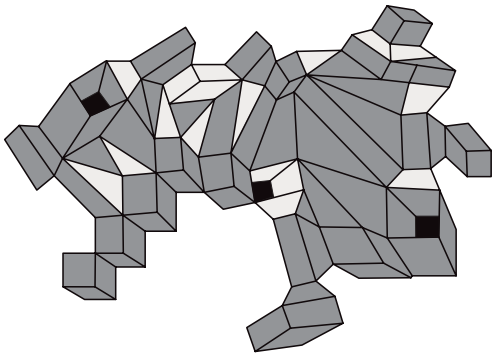
Una demostración alternativa de la parte (b) del teorema anterior, usando el método directo, es la siguiente:

Prueba. Dado un x cualquiera, tenemos:

$$\begin{aligned} x \in (A \cap B)^c &\leftrightarrow \neg(x \in A \cap B) && \text{(df. comp.)} \\ &\leftrightarrow \neg(x \in A \wedge x \in B) && \text{(df. inters.)} \\ &\leftrightarrow \neg(x \in A) \vee \neg(x \in B) && \text{(lógica)} \\ &\leftrightarrow (x \in A^c) \vee (x \in B^c) && \text{(df. comp.)} \\ &\leftrightarrow x \in A^c \cup B^c. && \text{(df. unión)} \end{aligned}$$

∎

Ejercicios



1. Sea $\mathcal{U} = \{x \in \mathbb{N} : x \leq 10\}$ y sean A, B y C los siguientes subconjuntos de $\mathcal{U}$: $A = \{1,4,5\}$, $B = \{4,6,7\}$ y $C = \{2,7,8\}$.
   Calcule los siguientes conjuntos, donde el complemento se toma con respecto a $\mathcal{U}$:

   (a) $A \cup B$,
   (b) $A \cap B$,
   (c) $A \cap C$,
   (d) $A \setminus C^c$,
   (e) $B \setminus C$,
   (f) $A \setminus (B \cap C)$,
   (g) B^c,
   (h) $(B \cup C)^c$,
   (i) $B^c \cup C^c$,
   (j) $\mathcal{P}(A \cup B)$,
   (k) $\mathcal{P}(A) \cup \mathcal{P}(B)$,
   (l) $C \setminus \mathcal{U}$.

2. Encuentre conjuntos A, B y C tales que $A \cap B \neq \varnothing$, $A \cap C \neq \varnothing$ y $B \cap C \neq \varnothing$, pero aun así $A \cap B \cap C = \varnothing$.
3. Demuestre que dados x y A se tiene:
   (a) $x \in A$ si y sólo si $A = A \cup \{x\}$.
   (b) $x \notin A$ si y sólo si $A = A \setminus \{x\}$.
4. Sean A y B conjuntos. Demuestre las siguientes afirmaciones:
   (a) $B \setminus A = B$ si y sólo si $A \setminus B = A$.
   (b) $A \cup B \subseteq A \cup B \cup C$.
   (c) $A \cap B \cap C \subseteq A \cap B$.
   (d) $A, B \subseteq C$ si y sólo si $A \cup B \subseteq C$.
   (e) $A, B \supseteq C$ si y sólo si $A \cap B \supseteq C$.
   (f) $A \cup B = A \cap B$ si y sólo si $A = B$.
   (g) si $B \nsubseteq A$ entonces $B \setminus A \neq \varnothing$;
   (h) $(A \cup B) \cap (C \cup B^c) \subseteq A \cup C$.

5. Dados los conjuntos A y B definimos su *diferencia simétrica* $A \triangle B$ de la siguiente manera:

$$A \triangle B := (A \cup B) \setminus (A \cap B).$$

Sean $A = \{1, 2, 3, 4\}$ y $B = \{0, 2, 4, 6\}$. Liste todos los elementos del conjunto $\mathcal{P}(A \triangle B)$.

6. Demuestre que A y B son disjuntos si y sólo si $A \cup B = A \triangle B$. (Véase el ejercicio 5 para la definición de $A \triangle B$.)

7. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:

   (a) $(A \setminus B)^c = \{x \in \mathcal{U} : x \in A \to x \notin B\}$.

   (b) $A \triangle B = \{x \in \mathcal{U} : x \in A \leftrightarrow x \notin B\}$. (Véase el ejercicio 5 para la definición de $A \triangle B$.)

8. Sean A, A', B y B' conjuntos tales que $A \subseteq A'$ y $B \subseteq B'$. Demuestre que si A' y B' son disjuntos, entonces A y B son disjuntos.

9. Sean $A, B \subseteq \mathcal{U}$, y sean $x, y \in \mathcal{U}$. Empareje cada afirmación de la izquierda con una de la derecha, de modo que sean equivalentes entre sí:

(1)	$\{x, y\} \setminus \{x\} = \varnothing$	(a)	$x \notin A$
(2)	$A^c = \varnothing$	(b)	$A = B = \varnothing$
(3)	$A \subseteq B$	(c)	$A \subseteq \{x\}$
(4)	$A \setminus \{x\} = \varnothing$	(d)	$\mathcal{P}(A) \subseteq \mathcal{P}(B)$
(5)	$\{x\} \neq \{y\}$	(e)	$x = y$
(6)	$A \cup \{x\} = A$	(f)	$A^c \subseteq B^c$
(7)	$x \in \varnothing$	(g)	$A = \{\varnothing\}$
(8)	$A \cup B = \varnothing$	(h)	$\mathcal{P}(A) = \{\varnothing\}$
(9)	$A \setminus \{x\} = A$	(i)	$\{x\} \cap \{y\} = \varnothing$
(10)	$A \cap B = \varnothing$	(j)	$\mathcal{P}(\varnothing) = \{\}$
(11)	$A^c = \mathcal{U} \setminus \{\varnothing\}$	(k)	$x \in A$
(12)	$A = \varnothing$	(l)	$A \subseteq B^c$
(13)	$A \cap B = B$	(m)	$A = \mathcal{U}$

10. Sean A y B conjuntos. Demuestre las siguientes afirmaciones:

    (a) Existe un conjunto C tal que $C \subseteq A$ y $A \setminus B = A \setminus C$.

    (b) Existe un conjunto C tal que A y C son disjuntos y se tiene que $A \cup B = A \cup C$.

    (c) Existe un conjunto C tal que $C \subseteq A$ son disjuntos y se tiene que $A \cap B = A \cap C$.

11. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:
    (a) Para todo conjunto X, si $X \cap B = X \cap C$, entonces $B = C$.
    (b) Si para todo conjunto X vale que $X \cap B = X \cap C$, entonces $B = C$.
    (c) Existe un conjunto X tal que, si $X \cap B = X \cap C$, entonces $B = C$.
    (d) Si existe un conjunto X tal que $X \cap B = X \cap C$, entonces $B = C$.
12. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:
    (a) Si $A \subseteq B$, entonces $A \cap (B \cup C) = A$.
    (b) $A \subseteq B$ si y sólo si $A \setminus B = \varnothing$.
    (c) $A \cap (B \cup C) \supseteq B \cup (A \cap C)$ si y sólo si $A \supseteq B$.
    (d) Si $A \cup B \cup C \subseteq \varnothing$, entonces $A = B = C = \varnothing$.
    (e) Si $A \cap B \cap C \subseteq \varnothing$, entonces $A = \varnothing$ o $B = \varnothing$ o $C = \varnothing$.
    (f) $A = B$ si y sólo si $A \setminus B = B \setminus A$.
    (g) Si $A^c \cap B^c = A^c \cup B^c$ entonces $A = B$.
13. Demuestre que $A \subseteq B \cup C$ si y sólo si existen A_1 y A_2, tales que $A_1 \subseteq B$, $A_2 \subseteq C$ y $A = A_1 \cup A_2$.
14. Diremos que *A muerde a B* si existe x tal que $x \in A$ y $x \in B$. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:
    (a) A muerde a A.
    (b) Si A muerde a B, entonces B muerde a A.
    (c) Si A muerde a B y B muerde a C, entonces A muerde a C.
    (d) Si A muerde a $B \cup C$, entonces A muerde a B o A muerde a C.
    (e) Si A muerde a B o A muerde a C, entonces A muerde a $B \cup C$.
    (f) Si A muerde a $B \cap C$, entonces A muerde a B y A muerde a C.
    (g) Si A muerde a B y A muerde a C, entonces A muerde a $B \cap C$.
    (h) Si $A \cup B$ muerde a C, entonces A muerde a C o B muerde a C.
15. Sean $A, B \subseteq \mathcal{U}$ conjuntos. Demuestre que las siguientes afirmaciones son equivalentes:
    (a) $A \subseteq B$.
    (b) Existe $\Delta \subseteq \mathcal{U}$ tal que $B \setminus \Delta = A$.

Concluya que el conjunto vacío es un subconjunto de todos los conjuntos. Ésta es una demostración natural de este hecho (compare con la demostración de la dirección $\rightarrow$ en el Teorema 1.14).

16. Demuestre el Teorema 1.25 (b).
17. Sean A y B conjuntos. Demuestre las siguientes propiedades (considere el Teorema 1.23):
    (a) $A \cap A = A$.
    (b) $A \cup B = B \cup A$.
    (c) $A \cap B \subseteq A \cup B$.
    (d) $A \cap \mathcal{U} = A$.
    (e) $(A \cap B) \cap C = A \cap (B \cap C)$.
18. Sean $A, B \subseteq \mathcal{U}$ conjuntos. Demuestre que las siguientes afirmaciones son equivalentes:
    (a) $A \subseteq B$.
    (b) $B^c \cap A = \varnothing$.
    (c) $A^c \cup B = \mathcal{U}$.
    (d) $B^c \subseteq A^c$.
    (e) $A \cap B = A$.
    (f) $A \cup B = B$.

    (*Ayuda*: demuestre que (a) implica (b), (b) implica (c), (c) implica (d), (d) implica (e), (e) implica (f) y (f) implica (a).)
19. Dado un conjunto $A \subseteq \mathcal{U}$, definimos $S(A)$ como el conjunto de los *singletons* que son subconjuntos de A, es decir:

$$S(A) := \{\{a\} : a \in A\}.$$

    En otras palabras, $x \in S(A)$ si y sólo si existe $a \in A$ tal que $x = \{a\}$. Demuestre las siguientes afirmaciones:
    (a) $S(A \cup B) = S(A) \cup S(B)$.
    (b) $S(A \cap B) = S(A) \cap S(B)$.
    (c) $S(\mathcal{U} \setminus A) = S(\mathcal{U}) \setminus S(A)$.
    (d) Si $S(A) = S(B)$, entonces $A = B$.
20. Sean A, B, C conjuntos. Demuestre las siguientes afirmaciones:
    (a) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
    (b) $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \cup \mathcal{P}(B)$. Además dé un ejemplo en el cual la contenencia anterior sea estricta.
    (c) $A = \varnothing$ si y sólo si $\mathcal{P}(A) = \{\varnothing\}$.
    (d) A y B son disjuntos si y sólo si $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\varnothing\}$.
    (e) Si $A \subseteq B$ y $A \subseteq C$, entonces

$$\{X \cap A : X \in \mathcal{P}(B)\} = \{X \cap A : X \in \mathcal{P}(C)\} = \mathcal{P}(A).$$

21. Compare las siguientes parejas de conjuntos de acuerdo con la relación $\subseteq$ (piense antes en ejemplos con conjuntos pequeños y después intente demostrar en general las contenencias que cree que siempre valen):

(a) $\mathcal{P}(\mathcal{U} \setminus A)$ vs. $\mathcal{P}(\mathcal{U}) \setminus \mathcal{P}(A)$;

(b) $\mathcal{P}(A \triangle B)$ vs. $\mathcal{P}(A) \triangle \mathcal{P}(B)$;

(c) $A \triangle (B \cup C)$ vs. $(A \triangle B) \cup (A \triangle C)$;

(d) $A \triangle (B \cap C)$ vs. $(A \triangle B) \cap (A \triangle C)$.

(Véase el ejercicio 5 para la definición de $A \triangle B$.)

22. Suponga que $A \subseteq B$, A tiene n elementos y B tiene m elementos. En términos de n y m, ¿cuántos elementos tiene $\{A \cup C : C \in \mathcal{P}(B)\}$?

23. Sean $A, B \subseteq \mathcal{U}$.

(a) Sea $\mathcal{F} = \{X \subseteq \mathcal{U} : A \subseteq X \text{ y } B \subseteq X\}$. Demuestre que $A \cup B$ es el *mínimo* elemento en $\mathcal{F}$ con respecto a la inclusión, es decir, demuestre que $A \cup B \in \mathcal{F}$ y que, para todo $X \in \mathcal{F}$, $A \cup B \subseteq X$.

(b) Sea $\mathcal{G} = \{X \subseteq \mathcal{U} : X \subseteq A \text{ y } X \subseteq B\}$. Demuestre que $A \cap B$ es el *máximo* elemento en $\mathcal{G}$ con respecto a la inclusión, es decir, demuestre que $A \cap B \in \mathcal{G}$ y que, para todo $X \in \mathcal{G}$, $X \subseteq A \cap B$.

(c) Sea $\mathcal{H} = \{X \subseteq \mathcal{U} : A \text{ y } X \text{ son disjuntos}\}$. Demuestre que el conjunto $A^c = \mathcal{U} \setminus A$ es el *máximo* elemento en $\mathcal{H}$ con respecto a la inclusión, es decir, demuestre que $A^c \in \mathcal{H}$ y que, para todo $X \in \mathcal{H}$, $X \subseteq A^c$.

24. Para este ejercicio considere las siguientes tres definiciones:

Definición (filtro). Sea X un conjunto no vacío. Un *filtro* sobre X es un conjunto $\mathcal{F} \subseteq \mathcal{P}(X)$ que cumple las siguientes propiedades:

(i) $\mathcal{F} \neq \varnothing$;

(ii) $\mathcal{F}$ es cerrado bajo la operación de intersección: si $S_1, S_2 \in \mathcal{F}$, entonces $S_1 \cap S_2 \in \mathcal{F}$;

(iii) $\mathcal{F}$ es cerrado bajo la relación de superconjunto: si $S_1 \subseteq S_2 \subseteq X$, y $S_1 \in \mathcal{F}$, entonces $S_2 \in \mathcal{F}$.

Definición (El filtro de Fréchet). Sea $\mathcal{F} = \{S \in \mathcal{P}(\mathbb{N}) : S^c \text{ es un conjunto finito}\}$ (aquí $\mathcal{U} = \mathbb{N}$, de modo que $S^c = \mathbb{N} \setminus S$). Por ejemplo, $\mathbb{N}^{>3} \in \mathcal{F}$ dado que $(\mathbb{N}^{>3})^c = \{0, 1, 2, 3\}$ es un conjunto finito; pero, para todo $n \in \mathbb{N}$, tenemos que

$$n\mathbb{N} = \{nx : x \in \mathbb{N}\} = \{0, n, 2n, \dots\};$$

luego $n\mathbb{N} \notin \mathcal{F}$.

Definición (ultrafiltro). Un filtro $\mathcal{F}$ sobre X es un *ultrafiltro* si para todo $A \subseteq X$ se tiene que $A \in \mathcal{F}$ o $A^c \in \mathcal{F}$.

Ahora bien:

(a) Demuestre que $\mathcal{F}$ es un filtro sobre el conjunto de los números naturales.

(b) Dé un ejemplo de un filtro $\mathcal{E}$ sobre $\mathbb{N}$, distinto del filtro de Fréchet.

(c) ¿Es el ejemplo que usted dio un ultrafiltro? ¿Es el filtro de Fréchet un ultrafiltro?

25. Sea B un subconjunto infinito de $\mathbb{N}$ y sea

$$I := \{A : A \subseteq \mathbb{N} \text{ y } A \cap B \text{ es finito}\}.$$

(a) Demuestre que $I \neq \varnothing$ y que $I \neq \mathcal{P}(\mathbb{N})$.

(b) Demuestre que I es *cerrado bajo uniones finitas*. En otras palabras, si $A, A' \in I$, entonces $A \cup A' \in I$.

(c) Demuestre que I es *cerrado bajo subconjunto*. En otras palabras, si $A \in I$ y $C \subseteq A$, entonces $C \in I$.

26. Para este ejercicio considere la siguiente definición:

Definición (ideal). Sea X un conjunto no vacío. Un *ideal* sobre X es un conjunto $\mathcal{F} \subseteq \mathcal{P}(X)$ que cumple las siguientes propiedades:

(i) $\mathcal{F} \neq \varnothing$;

(ii) $\mathcal{F}$ es cerrado bajo la operación de unión: si $S_1, S_2 \in \mathcal{F}$, entonces el conjunto $S_1 \cup S_2 \in \mathcal{F}$;

(iii) $\mathcal{F}$ es cerrado bajo la relación de subconjunto: si $S_1 \subseteq S_2$ y $S_2 \in \mathcal{F}$, entonces el conjunto $S_2 \in \mathcal{F}$.

(Note que el ejemplo dado en el ejercicio 25 es un ideal sobre $\mathbb{N}$.)

Ahora bien:

(a) Sea X un conjunto no vacío y sea $A \subseteq X$. Demuestre que el conjunto $\mathcal{F}_A := \{B \in \mathcal{P}(X) : B \subseteq A\}$ es un ideal sobre X.

(b) Demuestre que para todo $\mathcal{F} \subseteq \mathcal{P}(X)$ se tiene que $\mathcal{F}$ es un filtro, si y sólo si $\mathcal{P}(X) \setminus \mathcal{F}$ es un ideal.

27. Dados $A, B \subseteq \mathcal{U}$ conjuntos definimos $Z(A, B)$ como el siguiente conjunto:

$$Z(A, B) := \{x \in \mathcal{U} : \text{ si } x \in A, \text{ entonces } x \in B\}.$$

Demuestre las siguientes propiedades:

(a) $Z(A, A) = \mathcal{U}$.
(b) $Z(A, A \cup B) = \mathcal{U}$.
(c) $Z(A \cap B, A) = \mathcal{U}$.
(d) $Z(A, A^c) = \varnothing$.
(e) $Z(A, B) = Z(B^c, A^c)$.
(f) $Z(\varnothing, A) = \mathcal{U}$.
(g) $Z(A, \varnothing) = A^c$.
(h) $Z(A, B)^c = A \cap B^c$.
(i) $Z(A, B) = A^c \cup B$.

§ 1.4 Álgebra de conjuntos: pruebas sin doble inclusión

Recordemos algunas de las propiedades básicas que hemos establecido sobre las operaciones entre conjuntos:

Teorema 1.35. Dados los conjuntos $A, B, C \subseteq \mathcal{U}$, tenemos:[11]

(α_1) *Conmutatividad:* $\begin{cases} A \cup B = B \cup A; \\ A \cap B = B \cap A. \end{cases}$ (1.23 (b))

(α_2) *Asociatividad:* $\begin{cases} A \cup (B \cup C) = (A \cup B) \cup C; \\ A \cap (B \cap A) = (A \cap B) \cap C. \end{cases}$ (1.23 (f))

(α_3) *Absorción:* $\begin{cases} A \cap (A \cup B) = A; \\ A \cup (A \cap B) = A. \end{cases}$ (1.26)

(α_4) *Distribución:* $\begin{cases} A \cap (B \cup C) = (A \cap B) \cup (A \cap C); \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \end{cases}$ (1.25)

(α_5) *Todo o nada:* $\begin{cases} A \cap A^c = \varnothing; \\ A \cup A^c = \mathcal{U}. \end{cases}$ (1.32)

(α_6) *Identidad*: $\begin{cases} A \cup \varnothing = A; \\ A \cap \mathcal{U} = A. \end{cases}$ (1.23 (d))

(α_7) *Piso, techo:* $\begin{cases} A \cap \varnothing = \varnothing; \\ A \cup \mathcal{U} = \mathcal{U}. \end{cases}$ (1.23 (e))

(α_8) *Idempotencia:* $\begin{cases} A \cup A = A; \\ A \cap A = A. \end{cases}$ (1.23 (a))

(α_9) *Doble complemento:* $(A^c)^c = A$. (1.33 (b))

(α_{10}) *De Morgan:* $\begin{cases} (A \cup B)^c = A^c \cap B^c; \\ (A \cap B)^c = A^c \cup B^c. \end{cases}$ (1.34)

[11] Hacia la derecha referimos el número del teorema que le corresponde.

Para demostrar una igualdad de conjuntos podemos utilizar, como lo hemos hecho hasta ahora, el método de doble inclusión o el método directo. Sin embargo, existe otro procedimiento, llamado *álgebra de conjuntos*, que consiste en demostrar la igualdad de ambos conjuntos por medio de propiedades ya establecidas.

Álgebra de conjuntos

Veamos cómo puede hacerse esto:

Ejemplo 1.36. Demuestre mediante álgebra de conjuntos que

$$A = (A \cap B) \cup (A \cap B^c).$$

Solución.

$$\begin{aligned} A &= A \cap \mathcal{U} && \text{(Identidad, 1.23)} \\ &= A \cap (B \cup B^c) && \text{(Todo o nada, 1.32)} \\ &= (A \cap B) \cup (A \cap B^c) && \text{(Distribución, 1.25 (a))} \end{aligned}$$

■

En este esquema de prueba se debe justificar cada igualdad. Debe quedar claro que este método es igual de válido que los otros métodos discutidos en las secciones anteriores.

Ejemplo 1.37. Utilice el método de álgebra de conjuntos y las propiedades α_1 hasta α_5 para demostrar la propiedad α_6.

Solución. Veamos primero que $A \cup \varnothing = A$:

$$\begin{aligned} A &= A \cup (A \cap A^c) && \text{(Abs.)} \\ &= A \cup \varnothing. && \text{(Todo o nada)} \end{aligned}$$

Ahora veamos que $A \cap \mathcal{U} = A$:

$$\begin{aligned} A &= A \cap (A \cup A^c) && \text{(Abs.)} \\ &= A \cap \mathcal{U}. && \text{(Todo o nada)} \end{aligned}$$

■

El ejercicio 5 puede verse como una continuación de las ideas del ejemplo anterior.

Ejemplo 1.38. Demuestre mediante álgebra de conjuntos que

$$(A \cup B) \cap ((A \cup B) \cap (A \cap B)^c)^c = A \cap B.$$

Solución.

$$
\begin{aligned}
&(A \cup B) \cap ((A \cup B) \cap (A \cap B)^c)^c \\
&= (A \cup B) \cap ((A \cup B)^c \cup ((A \cap B)^c)^c) && \text{(De Morgan)} \\
&= (A \cup B) \cap ((A \cup B)^c \cup (A \cap B)) && \text{(Doble comp.)} \\
&= ((A \cup B) \cap (A \cup B)^c) \cup ((A \cup B) \cap (A \cap B)) && \text{(Dist.)} \\
&= \varnothing \cup ((A \cup B) \cap (A \cap B)) && \text{(Todo o nada)} \\
&= (A \cup B) \cap (A \cap B) && \text{(Conm. + Id.)} \\
&= ((A \cup B) \cap A) \cap B && \text{(Asoc.)} \\
&= A \cap B. && \text{(Conm. + Abs.)}
\end{aligned}
$$

■

Sean $A, B \subseteq \mathcal{U}$ conjuntos. Es fácil ver que si $A^c \cap B = \varnothing$, entonces $B \subseteq A$ y que si $A^c \cup B = \mathcal{U}$, entonces $A \subseteq B$ (véase el ejercicio 18). Concluimos por tanto que si $A^c \cap B = \varnothing$ y $A^c \cup B = \mathcal{U}$, entonces $A = B$. Este resultado lo podemos demostrar mediante álgebra de conjuntos:

Lema 1.39. Dados los conjuntos $A, B \subseteq \mathcal{U}$, tenemos:

$$\textit{si } A^c \cap B = \varnothing \text{ y } A^c \cup B = \mathcal{U}\textit{, entonces } A = B.$$

Prueba. Veamos primero que $A = A \cap B$:

$$
\begin{aligned}
A &= A \cap \mathcal{U} && \text{(Id.)} \\
&= A \cap (A^c \cup B) && \text{(Hipótesis)} \\
&= (A \cap A^c) \cup (A \cap B) && \text{(Dist.)} \\
&= \varnothing \cup (A \cap B) && \text{(Todo o nada)} \\
&= A \cap B. && \text{(Conm. + Id.)}
\end{aligned}
$$

Ahora veamos que $B = A \cap B$:

$$
\begin{aligned}
B &= B \cap \mathcal{U} && \text{(Id.)} \\
&= B \cap (A \cup A^c) && \text{(Todo o nada)} \\
&= (B \cap A) \cup (B \cap A^c) && \text{(Dist.)} \\
&= (A \cap B) \cup \varnothing && \text{(Conm. + Hipótesis)} \\
&= A \cap B. && \text{(Id.)}
\end{aligned}
$$

Entonces $A = A \cap B = B$. ■

Si utilizamos las propiedades α_1 hasta α_9 y el Lema 1.39 (que ha sido establecido utilizando algunas de estas propiedades), podemos dar

una prueba alternativa de la propiedad α_{10}, esto es, de las Leyes de De Morgan, mediante el álgebra de conjuntos:

Teorema 1.40 (Leyes de De Morgan). Para $A, B \subseteq \mathcal{U}$:

$$\text{(a)}\ \ (A \cup B)^c = A^c \cap B^c; \qquad \text{(b)}\ \ (A \cap B)^c = A^c \cup B^c.$$

Prueba. Dejamos la prueba de (b) al lector (ejercicio 1), y demostramos solamente (a): supongamos que $X = (A \cup B)^c$ y $Y = A^c \cap B^c$. En virtud del Lema 1.39, basta demostrar que $X^c \cap Y = \varnothing$ y $X^c \cup Y = \mathcal{U}$. Esto lo hacemos por medio de álgebra de conjuntos:

$$\begin{aligned}
X^c \cap Y &= ((A \cup B)^c)^c \cap (A^c \cap B^c) \\
&= (A \cup B) \cap (A^c \cap B^c) && \text{(Doble comp.)} \\
&= (A \cap (A^c \cap B^c)) \cup (B \cap (A^c \cap B^c)) && \text{(Dist.)} \\
&= ((A \cap A^c) \cap B^c) \cup ((B \cap B^c) \cap A^c) && \text{(Conm. + Asoc.)} \\
&= (\varnothing \cap B^c) \cup (\varnothing \cap A^c) && \text{(Todo o nada)} \\
&= \varnothing \cup \varnothing && \text{(Piso, techo)} \\
&= \varnothing. && \text{(Id.)}
\end{aligned}$$

Ahora veamos que $X^c \cup Y = \mathcal{U}$:

$$\begin{aligned}
X^c \cup Y &= ((A \cup B)^c)^c \cup (A^c \cap B^c) \\
&= (A \cup B) \cup (A^c \cap B^c) && \text{(Doble comp.)} \\
&= ((A \cup B) \cup A^c) \cap ((A \cup B) \cup B^c) && \text{(Dist.)} \\
&= ((A \cup A^c) \cup B) \cap ((B \cup B^c) \cup A) && \text{(Conm. + Asoc.)} \\
&= (\mathcal{U} \cup B) \cap (\mathcal{U} \cup A) && \text{(Piso, techo)} \\
&= \mathcal{U} \cap \mathcal{U} && \text{(Todo o nada)} \\
&= \mathcal{U}. && \text{(Id.)}
\end{aligned}$$

■

Propiedades duales

Propiedad dual

El *dual* de una propiedad P es la propiedad P^d que se consigue si intercambiamos $\cap$ por $\cup$, $\subseteq$ por $\supseteq$, $\mathcal{U}$ por $\varnothing$, y viceversa. Por ejemplo, el dual de la propiedad $P := A \cap B \subseteq A$ es $P^d := A \cup B \supseteq A$ y el dual de $P := A \cap \varnothing = \varnothing$ es $P^d := A \cup \mathcal{U} = \mathcal{U}$. La propiedad $A \subseteq \mathcal{U}$ es siempre válida y su dual $A \supseteq \varnothing$ también lo es. Las Leyes de Distribución son duales entre sí.

Veamos un ejemplo en donde utilizamos el álgebra de conjuntos para demostrar el dual de una propiedad válida. A partir de la ley de De

Morgan, a saber, $P := [(A \cap B)^c = A^c \cup B^c]$, podemos demostrar su dual, el cual es:

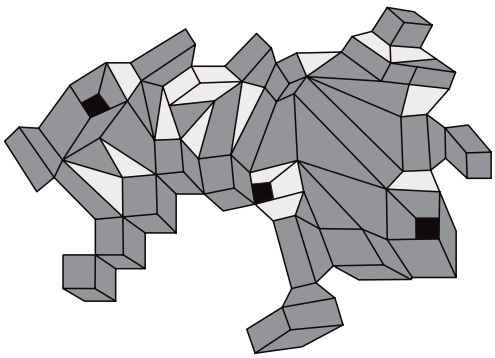
$$P^d := (A \cup B)^c = A^c \cap B^c.$$

Prueba.

$$\begin{aligned}(A \cup B)^c &= ((A^c)^c \cup (B^c)^c)^c && \text{(Doble comp.)}\\ &= ((A^c \cap B^c)^c)^c && \text{(Propiedad } P\text{)}\\ &= A^c \cap B^c. && \text{(Doble comp.)}\end{aligned}$$

■

Ejercicios



1. Demuestre que $(A \cup B)^c = A^c \cap B^c$ mediante el método de doble inclusión, y que $(A \cap B)^c = A^c \cup B^c$ mediante el método de álgebra de conjuntos.
2. Demuestre las siguientes propiedades de operaciones entre conjuntos mediante el método por elementos o álgebra de conjuntos:
   (a) $A \setminus (A \setminus B) = A \cap B$.
   (b) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.
   (c) $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$.
   (d) $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$.
   (e) $C \setminus (B \setminus A) = (A \cap C) \cup (C \setminus B)$.
   (f) $(B \setminus A) \cap C = (B \cap C) \setminus A = B \cap (C \setminus A)$.
   (g) $(B \setminus A) \cup C = (B \cup C) \setminus (A \setminus C)$.

3. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:
   (a) $(A \cup B) \cap C = A \cup (B \cap C)$.
   (b) $(A \cup B) \setminus A = B \setminus A$.
   (c) $(A \setminus B) \setminus C = A \setminus (B \cup C)$.
   (d) $A \setminus (B \setminus C) = (A \setminus B) \setminus C$.

4. Recordemos que, dados los conjuntos A y B, definimos su *diferencia simétrica* $A \triangle B$ así:
$$A \triangle B := (A \setminus B) \cup (B \setminus A).$$
   (a) Demuestre que $A \triangle B = (A \cap B^c) \cup (B \cap A^c)$.
   (b) Demuestre que $A \triangle B = (A \cup B) \setminus (A \cap B)$.
   (c) Demuestre que la operación $\triangle$ es conmutativa y asociativa.
   (d) ¿Qué conjunto es $A \triangle \varnothing$? ¿Y $A \triangle A$? ¿Y $A \triangle \mathcal{U}$?
   (e) Si $A \subseteq B$, ¿qué conjunto es $A \triangle B$?
   (f) Demuestre que $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.
   (g) Demuestre que $A \cup (B \triangle C) = A \triangle (B \setminus (A \cup C)) \triangle (C \setminus (A \cup B))$.
   (h) Demuestre que $(A \triangle B)^c = (A \cap B) \cup (A \cup B)^c$.
   (i) Demuestre que $A = B$ si y sólo si $A \triangle B = \varnothing$.
   (j) Demuestre que $B = ((A \triangle B) \cap A^c) \cup ((A \triangle B)^c \cap A)$.
   (k) Demuestre que si $A \triangle C = A \triangle B$ entonces $B = C$.
   (l) Demuestre que $A \cup B = (A \triangle B) \triangle (A \cap B)$.

5. Sean $\alpha_1, \alpha_2, \ldots, \alpha_{10}$ las propiedades listadas en el Teorema 1.35.
   (a) Utilice el método de álgebra de conjuntos y las propiedades α_1 hasta α_6 para demostrar la propiedad α_7.
   (b) Utilice el método de álgebra de conjuntos y las propiedades α_1 hasta α_7 para demostrar la propiedad α_8.
   (c) Utilice el método de álgebra de conjuntos y las propiedades α_1 hasta α_8 para demostrar la propiedad α_9.

6. Sean $A_1, A_2, A_3 \subseteq \mathcal{U}$. Demuestre las siguientes igualdades:
   (a) $A_1 \cup A_2 = (A_1 \setminus A_2) \cup (A_2 \setminus A_1) \cup (A_1 \cap A_2)$. Ilustre esta igualdad mediante un diagrama de Venn.
   (b) $(A_1 \cup A_2 \cup A_3)^c = A_1^c \cap A_2^c \cap A_3^c$.
   (c) $(A_1^c \cup A_2 \cup A_3^c)^c \cup A_3^c \cup A_1^c \cup A_2 = \mathcal{U}$.
   (d) $((A_1^c \cup A_2)^c \cup A_2)^c \cup (A_2^c \cup A_1)^c \cup A_1 = \mathcal{U}$.

(e) $(A \triangle B) \triangle (B \triangle C) \triangle (C \triangle D) = A \triangle D$.

(f) $(A \triangle B) \cup (A \triangle C) \cup (C \triangle D) = (A \cup B \cup C \cup D) \setminus (A \cap B \cap C \cap D)$.

7. Demuestre mediante doble inclusión o álgebra de conjuntos que
$$A^c \cap (B \triangle C) = [B \setminus (A \cup C)] \cup [C \setminus (A \cup B)].$$

8. Definimos así la operación L (donde se tiene que $A, B, C \subseteq \mathcal{U}$):
$$L(A, B, C) = (A \cap B) \cup (B \cap C) \cup (A \cap C).$$
Demuestre las siguientes propiedades:

(a) $L(A, B, C) = L(A, C, B) = L(B, A, C)$.

(b) $L(A, A, A) = A$.

(c) $L(A, B, \varnothing) = A \cap B$.

(d) $L(\mathcal{U}, A, B) = A \cup B$.

(e) $L(A \cup B, B, C) = L(A, B, C) \cup B$.

(f) $L(A \cap B, B, C) = (A \cup C) \cap B$.

(g) A, B y C son conjuntos disjuntos dos a dos,[12] si y sólo si se tiene que $L(A, B, C) = \varnothing$.

(h) $L(A, B, C) = \mathcal{U}$ si y sólo si $\{A, B\} = \{\mathcal{U}\}$ o $\{B, C\} = \{\mathcal{U}\}$ o $\{A, C\} = \{\mathcal{U}\}$.

(i) $L(A, B, C) = A$ si y sólo si $B \cap C \subseteq A \subseteq B \cup C$.

(j) Si $A \subseteq B \subseteq C$, entonces $L(A, B, C) = A \cup B$.

(k) Si $A_1 \subseteq B_1$, $A_2 \subseteq B_2$ y $A_3 \subseteq B_3$, entonces se puede concluir que $L(A_1, A_2, A_3) \subseteq L(B_1, B_2, B_3)$.

(l) $L(A, A^c, B) = B$.

(m) $L(A_1^c, A_2^c, A_3^c) = \{x \in \mathcal{U} :$ si $x \in A_i$, entonces se puede concluir que $x \notin A_j \cup A_k, \{i, j, k\} = \{1, 2, 3\}\}$.

9. Sea $M(A, B, C) = (A \cup B \cup C) \setminus L(A, B, C)$ (véase el ejercicio 8). Demuestre que
$$M(A, B, C) = (A \cap B^c \cap C^c) \cup (B \cap C^c \cap A^c) \cup (C \cap A^c \cap B^c).$$

10. En este ejercicio demostraremos que con las operaciones de complemento y unión podemos expresar las demás operaciones conjuntistas. Sean $A, B \subseteq \mathcal{U}$. Utilizando únicamente las operaciones de complemento respecto de $\mathcal{U}$ y unión, exprese los siguiente conjuntos:
$$\text{(a) } A \cap B, \qquad \text{(b) } A \triangle B, \qquad \text{(c) } A \setminus B.$$

[12] Esto quiere decir que $A \cap B = B \cap C = A \cap C = \varnothing$.

11. En este ejercicio demostraremos que con las operaciones de complemento y diferencia simétrica podemos expresar las demás operaciones conjuntistas. Sean $A, B \subseteq \mathcal{U}$. Utilizando únicamente las operaciones de complemento respecto de $\mathcal{U}$ y diferencia simétrica, exprese los siguiente conjuntos:

    (a) $A \cup B$, (b) $A \cap B$, (c) $A \setminus B$.

12. Para este ejercicio considere la siguiente definición:

    Definición. Sean A_1, A_2 y A_3 conjuntos cualesquiera. Dado un conjunto X, diremos que X es *aglomerado* si, para toda elección de índices distintos entre sí i, j, k entre 1 y 3 (dicho de otro modo, $\{1,2,3\} = \{i,j,k\}$), se cumplen las siguientes propiedades:

    (i) $\varnothing \subseteq X \subseteq A_1 \cup A_2 \cup A_3$;

    (ii) si $X \cap A_i \neq \varnothing$, entonces $X \supseteq A_i \setminus (A_j \cup A_k)$;

    (iii) si $X \cap A_i \neq \varnothing$ y $X \cap A_j \neq \varnothing$, entonces $X \supseteq (A_i \cap A_j) \setminus A_k$;

    (iv) si $X \cap A_i \neq \varnothing$, $X \cap A_j \neq \varnothing$ y $X \cap A_k \neq \varnothing$, entonces $X \supseteq A_i \cap A_j \cap A_k$.

    Ahora bien:

    (a) Sea $\mathcal{A} = \{X : X \text{ es un conjunto aglomerado}\}$ y k el número de elementos de $\mathcal{A}$ (k puede ser en principio infinito). Calcule *todos* los distintos valores que k puede tomar, al hacer variar los conjuntos A_1, A_2 y A_3. (Por ejemplo, si $A_1 = A_2 = A_3 = \varnothing$, el único conjunto aglomerado es $\varnothing$.)

    (b) Si se trabaja ahora únicamente con dos conjuntos base A_1 y A_2, idee una definición de conjunto aglomerado análoga a la anterior, y calcule el número máximo posible de conjuntos aglomerados.

§ 1.5 Unión e intersección generalizadas

En esta sección generalizaremos las operaciones de unión e intersección de conjuntos. La generalización consiste en que en vez de unir únicamente dos conjuntos, podremos unir cualquier número de conjuntos, incluso un número infinito de ellos. De forma análoga procederemos con la intersección.

Imaginemos un conjunto A como una caja cuyos elementos son bolsas $b \in A$, cada una de las cuales tiene ciertas piedras $p \in b$. A partir de esto podemos formar el conjunto que resulta de introducir todas estas piedras en una nueva caja:

Definición 1.41 (Unión generalizada). Sea A un conjunto. Definimos $\bigcup A$ (la *unión de A*) así: *Unión generalizada*

$$\forall p : p \in \bigcup A \leftrightarrow \exists b \in A : p \in b.$$

Es decir,

$$\bigcup A := \{p : \text{ existe } b \in A, \text{ tal que } p \in B\}.$$

Ilustremos los anterior con una analogía: una piedra $p \in \bigcup A$ si y sólo si existe una bolsa b perteneciente a la caja A, tal que p pertenece a b. Un caso particular de esto es cuando la caja A tiene como elementos exactamente a las bolsas B y C: $A = \{B, C\}$. Es claro entonces que $x \in \bigcup A$ si y sólo si $x \in B \vee x \in C$; en otras palabras, $\bigcup A$ coincide con el conjunto $B \cup C$.

De forma análoga podemos definir la intersección generalizada:

Definición 1.42 (Intersección generalizada). Sea A un conjunto. Definimos $\bigcap A$ (la *intersección de A*) así: *Intersección generalizada*

$$\forall p : p \in \bigcap A \leftrightarrow \forall b \in A : p \in b.$$

Es decir,

$$\bigcap A := \{p : \text{ para todo } b \in A, p \in B\}.$$

Ejemplo 1.43.

(a) Si $A = \{\{1,2\},\{2,4\},\{2,4,8\}\}$, entonces:

$$\bigcup A = \{1,2\} \cup \{2,4\} \cup \{2,4,8\} = \{1,2,4,8\};$$
$$\bigcap A = \{1,2\} \cap \{2,4\} \cap \{2,4,8\} = \{2\}.$$

(b) Si $A = \{\mathbb{N}, \{-3,-2,-1,0,1\}, \{-1,0,1,2,3\}\}$, entonces:

$$\bigcup A = \{n \in \mathbb{Z} : n \geq 3\} \text{ y } \bigcap A = \{0,1\}.$$

(c) Para todo $n \in \mathbb{N}$, sea $A_n = \{0,1,n\}$. Por ejemplo, $A_0 = \{0,1\}$ y $A_5 = \{0,1,5\}$. Sea $A = \{A_n : n \in \mathbb{N}\}$. Entonces puede verse que

$$\bigcup A = \mathbb{N} \text{ y } \bigcap A = \{0,1\}.$$

Demostremos que $\bigcap A = \{0,1\}$.

Solución. Para ello utilizamos el método de doble inclusión:

($\subseteq$) Sea $x \in \bigcap A$. Esto implica que para todo $b \in A$, $x \in b$. En particular, como $A_0 \in A$, se tiene que $x \in A_0$. Entonces $x \in \{0,1\}$.

(⊇) Sea $x \in \{0,1\}$. Queremos ver que $x \in \bigcap A$, es decir, que para todo $b \in A$, $x \in b$. Sea $b \in A$: entonces existe $n \in \mathbb{N}$ tal que $b = A_n = \{0,1,n\}$. Entonces claramente $x \in b$, como queríamos. Esto prueba que $x \in \bigcap A$. ∎

Teorema 1.44. Sean A y B conjuntos. Tenemos:

(a) *monotonía*: $A \subseteq B$ implica $\bigcup A \subseteq \bigcup B$;

(b) $B \subseteq A$ implica $\bigcap A \subseteq \bigcap B$.

Prueba.

(a) Si $x \in \bigcup A$, entonces $x \in y$ para algún $y \in A$. Como $A \subseteq B$, entonces y también pertenece a B, y así $x \in y$ para algún $y \in B$, esto es, $x \in \bigcup B$.

(b) Si $x \in \bigcap A$, entonces para todo $y \in A$, $x \in y$. Como $B \subseteq A$, entonces para todo $y \in B$, $x \in y$, esto es, $x \in \bigcap B$. ∎

Teorema 1.45. Sea A un conjunto no vacío. Entonces:

(a) si $a \in A$, entonces $a \subseteq \bigcup A$;

(b) si $a \in A$, entonces $\bigcap A \subseteq a$;

(c) si para todo $a \in A$ se tiene que $c \subseteq a$, entonces $c \subseteq \bigcap A$;

(d) si para todo $a \in A$ se tiene que $a \subseteq c$, entonces $\bigcup A \subseteq c$.

Prueba. Se deja al lector (ejercicio 7 (h)). ∎

Índices

Sea I un conjunto y para todo $i \in I$ sea A_i un conjunto. Entonces podemos definir un conjunto A que contiene como elementos precisamente *todos* los conjuntos A_i, esto es,

$$A = \{A_i : i \in I\}.$$

Índices El conjunto I se denomina *conjunto de índices*. Con base en el conjunto A cuyos elementos son los conjuntos A_i ($i \in I$), definimos:

$$\bigcup_{i \in I} A_i := \bigcup A, \text{ que se lee: "la unión de los } A_i \text{ con } i \in I\text{"},$$

$$\bigcap_{i \in I} A_i := \bigcap A, \text{ que se lee: "la intersección de los } A_i \text{ con } i \in I\text{"}.^{13}$$

[13] Es usual hallar estos conjuntos simbolizados con sus índices hacia la derecha, en el siguiente modo: $\bigcup_{i \in I} A_i$ y $\bigcap_{i \in I} A_i$.

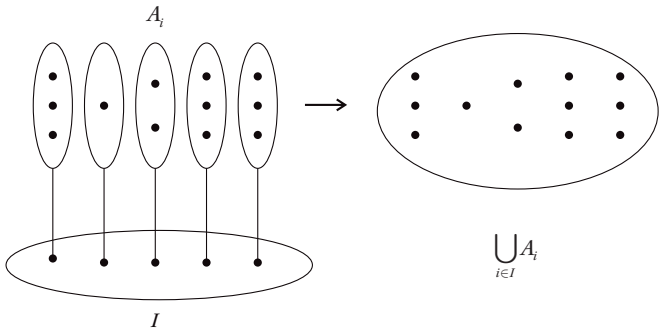


Figura 1.5: La unión de los A_i con $i \in I$.

Para los siguientes ejemplos es necesario introducir al conjunto de los *números reales*, $\mathbb{R}$. La definición precisa de este conjunto no es tan sencilla. Intuitivamente el conjunto de los números reales se representa por una recta infinita "sin huecos", e incluye, por ejemplo, los números $-7, 3, -1, \frac{1}{2}, \sqrt{2}, \pi, 14$, etc.

$\mathbb{R}$: *Números reales*

Por otro lado, el conjunto de los *números enteros* es el conjunto:

$$\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

$\mathbb{Z}$: *Números enteros*

Además, el conjunto de los *números racionales* es el conjunto:

$$\mathbb{Q} := \left\{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\right\}.$$

$\mathbb{Q}$: *Números racionales*

Entonces tenemos que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Definición 1.46. Sea $A \subseteq \mathbb{R}$ y sea $a \in \mathbb{R}$. Definimos los siguientes subconjuntos de A:

$A^{\leq a}$, A^*
$A^{\geq a}$, A^+
$A^{<a}$, A^-
$A^{>a}$

(a) $A^{\leq a} := \{x \in A : x \leq a\}$;
(b) $A^{\geq a} := \{x \in A : x \geq a\}$;
(c) $A^{<a} := \{x \in A : x < a\}$;
(d) $A^{>a} := \{x \in A : x > a\}$;
(e) $A^* := \{x \in A : x \neq 0\}$;
(f) $A^+ := A^{>0} = \{x \in A : x > 0\}$;
(g) $A^- := A^{<0} = \{x \in A : x < 0\}$.

Por ejemplo, $\mathbb{N}^* = \mathbb{N}^+ = \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, $\mathbb{N}^- = \varnothing$ y, en general se tiene que $A^* = A^+ \cup A^-$. Por definición, un número $x \in \mathbb{R}$ es *nulo* si $x = 0$; por ello, el conjunto A^* se llama el *conjunto de elementos no nulos de A*.

Ejemplo 1.47. Dado $n \in \mathbb{N}^*$ sea $A_n = [0, \frac{1}{n}]$. Demuestre entonces que $\bigcap_{n\in\mathbb{N}^*} A_n = \{0\}$.

Solución. Utilizamos el método de doble inclusión:

(⊆) Sea $x \in \bigcap_{n\in\mathbb{N}^*} A_n$. Entonces, para todo $n \in \mathbb{N}^*$, $x \in [0, \frac{1}{n}]$. Esto implica que

$$\forall n \in \mathbb{N}^* : 0 \leq x \leq \frac{1}{n}. \qquad (*)$$

En particular, se tiene que $0 \leq x$. Queremos ver que $x \in \{0\}$, es decir, que $x = 0$. Supongamos por contradicción que $x \neq 0$. Entonces $0 < x$. Sea m la parte entera de $\frac{1}{x}$, esto es, el máximo número natural m tal que $m \leq \frac{1}{x}$. Sea $n = m+1$. Entonces $n \in \mathbb{N}^*$ y $n > \frac{1}{x}$. Esto implica que $x > \frac{1}{n}$, luego $x \notin A_n$, lo cual contradice (*). Concluimos que $x = 0$, como se quería.

(⊇) Sea $x \in \{0\}$. Entonces $x = 0$, lo que implica que para todo $n \in \mathbb{N}$, $0 \leq x \leq \frac{1}{n}$. Entonces $x \in \bigcap_{n\in\mathbb{N}^*} A_n$. ∎

Ejemplo 1.48. Dado $i \in \mathbb{N}^*$, sea $A_i = (0, i) = \{x \in \mathbb{R} : 0 < x < i\}$ (el intervalo abierto entre 0 e i). Podemos afirmar que:

$$\bigcup_{i\in\mathbb{N}^*} A_i = \mathbb{R}^+, \qquad \bigcap_{i\in\mathbb{N}^*} A_i = (0, 1).$$

Estas dos igualdades se puede justificar informalmente así: si "unimos" todos los intervalos A_i, cubrimos a todos los números reales positivos. En contraste, si "intersecamos" todos los intervalos A_i, tan sólo quedan aquellos elementos $x \in \mathbb{R}$ tales que $0 < x < 1$, pues ellos son los únicos elementos que son comunes a todos los intervalos. El lector deberá formalizar los anteriores argumentos por medio de pruebas de igualdad de conjuntos (véase el ejercicio 3).

El Teorema 1.45 puede reformularse si utilizamos la terminología de subíndices:

Teorema 1.49. Sea $\{A_i : i \in I\}$ un conjunto. Entonces:

(a) para todo $j \in I$, $A_j \subseteq \bigcup_{i\in I} A_i$;

(b) para todo $j \in I$, $\bigcap_{i\in I} A_i \subseteq A_j$;

(c) si para todo $i \in I$, $C \subseteq A_i$, entonces $C \subseteq \bigcap_{i\in I} A_i$;

(d) si para todo $j \in I$, $A_j \subseteq C$, entonces $\bigcup_{i\in I} A_i \subseteq C$.

El resultado más importante que relaciona la unión con la intersección generalizada es el teorema de De Morgan generalizado:

Teorema 1.50 (De Morgan generalizado). Sea $A = \{A_i : i \in I\}$ un conjunto tal que, para todo $i \in I$, A_i es un conjunto tal que $A_i \subseteq \mathcal{U}$. Entonces:

$$\text{(a)}\ \left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c; \qquad \text{(b)}\ \left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c.$$

Prueba. Demostraremos la igualdad (a) por el método de doble inclusión y la igualdad (b) por el método directo:

(a) Si $x \in (\bigcap_{i\in I} A_i)^c$, entonces $x \notin \bigcap_{i\in I} A_i$, luego *no* es cierto que para todo $i \in I$ $x \in A_i$; por ende, debe existir un $i_0 \in I$ tal que $x \notin A_{i_0}$, es decir, $x \in A_{i_0}^c$. Pero, por el Teorema 1.49(a), $A_{i_0}^c \subseteq \bigcup_{i\in I} A_i^c$, luego $x \in \bigcup_{i\in I} A_i^c$. La otra inclusión se demuestra de forma análoga.

(b) Dado un x cualquiera, tenemos que

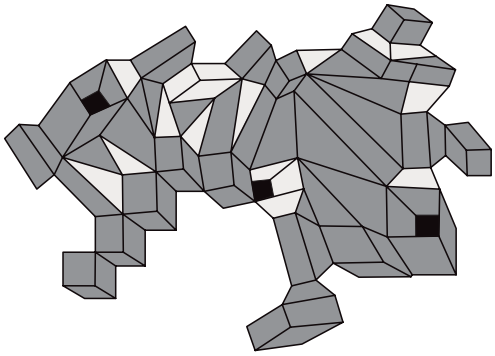
$$\begin{aligned}
x \in \left(\textstyle\bigcup_{i\in I} A_i\right)^c &\leftrightarrow x \notin \textstyle\bigcup_{i\in I} A_i && \text{(df. comp.)}\\
&\leftrightarrow \text{no existe } i \in I \text{ tal que } x \in A_i && \text{(df. unión gen.)}\\
&\leftrightarrow \text{para todo } i \in I, x \notin A_i && \text{(lógica)}\\
&\leftrightarrow \text{para todo } i \in I, x \in A_i^c && \text{(df. comp.)}\\
&\leftrightarrow x \in \textstyle\bigcap_{i\in I} A_i^c. && \text{(df. inters.)}
\end{aligned}$$

■

☞ **Antes de seguir leyendo**

1. Sea A un conjunto. ¿Qué conjunto es $\bigcup(\mathcal{P}(A))$? Y ¿$\bigcap(\mathcal{P}(A))$?
2. ¿Qué conjunto es $\bigcup\varnothing$?
3. ¿Verdadero o falso? $\forall A : \bigcap A \subseteq \bigcup A$.
4. ¿Qué es $\bigcap\varnothing$? Justifique.

Ejercicios



1. Compare las siguientes parejas de conjuntos de acuerdo con la relación $\subseteq$ (piense antes en ejemplos con conjuntos pequeños y después intente demostrar en general las contenencias que cree que siempre valen):
   (a) $\bigcap_{i\in I}(A\cup A_i)$ vs. $A\cup(\bigcap_{i\in I}A_i)$.
   (b) $(\bigcup_{i\in I}A_i)\setminus(\bigcup_{i\in I}B_i)$ vs. $\bigcup_{i\in I}(A_i\setminus B_i)$.
2. Demuestre el Teorema 1.45.
3. Dado $i\in\mathbb{N}^*$, sea $A_i=(0,i)$. Demuestre las siguientes afirmaciones:
   (a) $\bigcup_{i\in\mathbb{N}^*}A_i=\mathbb{R}^+$; (b) $\bigcap_{i\in\mathbb{N}^*}A_i=(0,1)$.
4. Sean A,B conjuntos, con $A\subseteq B$. Dado $x\in B$, sea $E_x=\{x\}$. ¿Qué conjunto es $\bigcup_{s\in A}E_s$? Demuestre su afirmación.
5. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso (suponga que $I\neq\varnothing$):
   (a) $B\setminus\bigcup_{i\in I}A_i=\bigcup_{i\in I}(B\setminus A_i)$;
   (b) $B\setminus\bigcup_{i\in I}A_i=\bigcap_{i\in I}(B\setminus A_i)$;
   (c) $(\bigcup_{i\in I}A_i)\setminus B=\bigcup_{i\in I}(A_i\setminus B)$;
   (d) $(\bigcap_{i\in I}A_i)\setminus B=\bigcap_{i\in I}(A_i\setminus B)$;
   (e) $B\setminus\bigcap_{i\in I}A_i=\bigcap_{i\in I}(B\setminus A_i)$;
   (f) $B\setminus\bigcap_{i\in I}A_i=\bigcup_{i\in I}(B\setminus A_i)$.
6. (a) ¿Qué conjunto es $A=\displaystyle\bigcup_{a\in[0,1)}\left(\bigcap_{b\in(a,6]}[b,b+a)\right)$?
   (b) Dado $i\in\mathbb{Z}$, sea $A_i=[2i,2i+1]$. ¿Qué conjunto es $\left(\bigcup_{i\in\mathbb{Z}}A_i\right)^c$?

7. Demuestre las siguientes igualdades de conjuntos:
   (a) $\varnothing = \bigcap_{B \in \mathcal{P}(A)} B$.
   (b) $A = \bigcup \mathcal{P}(A)$.
   (c) $\mathbb{R}^- = \bigcup_{a \in \mathbb{Z}^-} [a, a+1)$. (Aquí $[a, a+1) = \{x \in \mathbb{R} : a \leq x < a+1\}$.)
   (d) $\mathbb{R} = \bigcup_{x \in \mathbb{R}} \left(\bigcap_{\varepsilon > 0} (x - \varepsilon, x + \varepsilon) \right)$.
8. Para todo $n, m \in I$ sea $A_{n,m}$ un conjunto. Demuestre que
$$\left(\bigcup_{n \in I} \left(\bigcap_{m \in I} A_{n,m} \right) \right)^c = \bigcap_{n \in I} \left(\bigcup_{m \in I} A_{n,m}^c \right).$$
9. Demuestre que $A \subseteq \bigcup_{i \in I} B_i$ si y sólo si existen los conjuntos A_i ($i \in I$) tales que $A = \bigcup_{i \in I} A_i$ y, para todo $i \in I$, se tiene que $A_i \subseteq B_i$.
10. Demuestre mediante un contraejemplo que la siguiente afirmación no es válida en general: si $\bigcup A \subseteq \bigcup B$, entonces $A \subseteq B$.
11. Para todo $i \in I$ sea A_i un conjunto, y para todo $j \in J$ sea B_j un conjunto. Demuestre que, si para todo $i \in I$ y para todo $j \in J$ se tiene que $A_i \cap A_j = \varnothing$, entonces
$$\left(\bigcup_{i \in I} A_i \right) \cap \left(\bigcup_{i \in J} B_j \right) = \varnothing.$$
12. Sea A un conjunto. Dado $a \in A$, sea $E_a = \{B \in \mathcal{P}(A) : a \in B\}$. Demuestre mediante doble inclusión que $\bigcup_{a \in A} E_a = \mathcal{P}(A) \setminus \{\varnothing\}$ y $\bigcap_{a \in A} E_a = \{A\}$.

§ 1.6 Producto cartesiano

(a, b): *Par ordenado*

Un *par ordenado* (a, b) consiste en dos elementos a y b no necesariamente distintos, que aparecen en cierto orden: a aparece de primero y b de segundo. Por ejemplo, el par ordenado $(4, 6)$ es distinto del par $(6, 4)$, pues si bien ambos listan los mismos elementos, lo hacen en orden distinto. Es por esto que un par ordenado no es lo mismo que un conjunto de dos elementos; en los conjuntos no importa el orden en que se listen sus elementos y, por ejemplo, $\{4, 6\} = \{6, 4\}$, mientras que —como ya hemos explicado— $(4, 6) \neq (6, 4)$.

La definición conjuntista de un par ordenado (a, b) es poco útil y poco intuitiva para la teoría que queremos desarrollar, aunque por supuesto

la daremos más adelante en esta sección (Definición 1.54). A partir de ella se puede demostrar, como se quiere, que

$$(a,b) = (a',b') \text{ si y sólo si } a = a' \text{ y } b = b'.$$

☞ **Antes de seguir leyendo**

Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:

1. $(2,2)$ es un par ordenado.
2. $\{a,b\}$ es un conjunto de dos elementos.
3. $(3,3) = (3,5)$.
4. $((3,2),1) = ((3,2),1)$.
5. Si $(a,b) = (b,c)$, entonces $\{a,b,c\}$ es un *singleton*.

Si A y B son conjuntos, podemos definir el conjunto de todas las parejas ordenadas (a,b), donde a proviene de A, y b proviene de B. A este conjunto lo llamamos el *producto cartesiano* entre A y B y lo denotamos como $A \times B$. Formalmente:

$A \times B$: Producto cartesiano

Definición 1.51 (Producto cartesiano). $A \times B := \{(x,y) : x \in A, y \in B\}$.
Notación: $A^2 := A \times A = \{(x,y) : x,y \in A\}$.

Ejemplo 1.52. Ejemplos de productos cartesianos:

(a) Si $A = \{1,2\}$ y $B = \{-1,0,1\}$, entonces

$$A \times B = \{(1,-1),(1,0),(1,1),(2,-1),(2,0),(2,1)\}.$$

Note que el conjunto A tiene 2 elementos, el conjunto B tiene 3 elementos y el conjunto $A \times B$ tiene $2 \times 3 = 6$ elementos. De este hecho proviene la palabra "producto" en la definición.

(b) $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ es conocido como el *plano cartesiano*. Las caricaturas y los demás objetos bidimensionales pueden verse como subconjuntos de $\mathbb{R}^2$. Un círculo no es más que cierto subconjunto de $\mathbb{R}^2$; por ejemplo, el círculo de radio 3 centrado en

el origen, es decir, en $(0,0)$ es el siguiente conjunto de pares ordenados:

$$\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 9\} \subseteq \mathbb{R}^2.$$

Los objetos tridimensionales son subconjuntos de $\mathbb{R}^2 \times \mathbb{R}$, que llamamos $\mathbb{R}^3$ para abreviar.

Teorema 1.53 (Propiedades básicas del producto cartesiano). Dados los conjuntos A, A', B, B' y C se tiene:

(a) $A \times \varnothing = \varnothing \times B = \varnothing$;

(b) si A y B son conjuntos no vacíos, $A = B$ si y sólo si $A \times B = B \times A$;

(c) si A y B son conjuntos no vacíos, $A = A'$ y $B = B'$ si y sólo si $A \times B = A' \times B'$;

(d) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;

(e) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Prueba. Demostramos (b) y (d) y dejamos las partes (a), (c) y (e) al lector (ejercicio 5):

(a) Supongamos que A y B son conjuntos no vacíos. Utilizamos el método de doble implicación:

  ($\to$) Supongamos que $A = B$. Entonces $A \times B = A \times A = B \times A$.

  ($\leftarrow$) Supongamos que $A \times B = B \times A$. Debemos demostrar que $A = B$. Utilizamos el método de doble inclusión:

    ($\subseteq$) Sea $x \in A$. Como $B \neq \varnothing$, existe y tal que $y \in B$. Entonces por definición $(x,y) \in A \times B$. Por hipótesis $A \times B = B \times A$, entonces $(x,y) \in B \times A$, lo que implica que $x \in B$.

    ($\supseteq$) Es análoga.

(b) Utilizamos el método de doble inclusión:

  ($\subseteq$) Sea $(x,y) \in A \times (B \cup C)$. Entonces $x \in A$ y $y \in B \cup C$. Tenemos dos casos:

  (i) $y \in B$: en este caso concluimos que $(x,y) \in A \times B$.

  (ii) $y \in C$: en este caso concluimos que $(x,y) \in A \times C$.

  A partir del razonamiento anterior podemos concluir que $(x,y) \in A \times B$ o $(x,y) \in A \times C$; luego $(x,y) \in (A \times B) \cup (A \times C)$.

(⊇) Sea $(x,y) \in (A \times B) \cup (A \times C)$. Entonces hay dos casos:

(i) $(x,y) \in A \times B$: en este caso $x \in A$ y $y \in B$; como $B \subseteq B \cup C$, concluimos que $y \in B \cup C$ y, por lo tanto, se tiene que $(x,y) \in A \times (B \cup C)$.

(ii) $(x,y) \in A \times C$: mediante un razonamiento análogo al anterior se demuestra que $(x,y) \in A \times (B \cup C)$.

En cualquier caso concluimos que $(x,y) \in A \times (B \cup C)$, como queríamos. ∎

n-tupla

De forma análoga a la definición de un par ordenado, si n es un número natural positivo, podemos definir una *n-tupla* $(a_1, a_2, \ldots, a_n)$ como un objeto tal que:

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \leftrightarrow \forall i \in \{1, 2, \ldots, n\} : a_i = b_i.$$

Podemos generalizar el producto cartesiano entre dos conjuntos y definir el *producto cartesiano* entre n conjuntos $A_1, \ldots, A_n$, donde $n \in \mathbb{N}^*$ de la siguiente manera:

$$A_1 \times A_2 \cdots \times A_n := \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n\}.$$

Definición conjuntista de un par ordenado

En esencia, queremos definir (a,b) como un conjunto, en términos de a y b, que satisfaga la siguiente propiedad:

$$(a,b) = (a',b') \text{ si y sólo si } a = a' \text{ y } b = b'.$$

Definición 1.54 (Par ordenado). Dados a y b, definimos el *par ordenado* (a,b) así:

$$(a,b) := \{\{a\}, \{a,b\}\}.$$

Por ejemplo, $(4,6)$ es el conjunto $\{\{4\}, \{4,6\}\}$, mientras que $(6,4)$ es el conjunto $\{\{6\}, \{6,4\}\}$. Note que, por ejemplo, $\{4\} \in (4,6) \setminus (6,4)$ y por esto concluimos que $(4,6) \neq (6,4)$.

Antes de demostrar la propiedad que mencionamos anteriormente, vale la pena observar los siguientes hechos conjuntistas (cuya demostración dejamos al lector), que utilizaremos constantemente en su prueba:

(a) $a \neq b$ si y sólo si $\{a,b\}$ no es un *singleton*;

(b) $a = b$ si y sólo si $\{a\} = \{b\}$.

Teorema 1.55 (Propiedad del par ordenado). $(a,b) = (a',b')$ si y sólo si $a = a'$ y $b = b'$. *Propiedad del par ordenado*

Prueba. La dirección ← es inmediata por la definición de par ordenado. Demostremos la otra dirección: supongamos que $(a,b) = (a',b')$, esto es,

$$\{\{a\},\{a,b\}\} = \{\{a'\},\{a',b'\}\}.$$

Dividiremos la prueba en dos casos, según a' y b' sean iguales o no:

> (i) $a' = b'$: entonces
>
> $$\{\{a\},\{a,b\}\} = \{\{a'\},\{a',b'\}\} = \{\{a'\},\{a',a'\}\} = \{\{a'\},\{a'\}\} = \{\{a'\}\}.$$
>
> Entonces $\{a\} = \{a,b\} = \{a'\}$, lo cual implica que $a = b = a'$. Entonces a, a', b y b' son el mismo elemento, y en particular, podemos concluir $a = a'$ y $b = b'$.

> (ii) $a' \neq b'$: entonces $\{\{a'\},\{a',b'\}\}$ tiene dos elementos, lo cual implica que $\{\{a\},\{a,b\}\}$ (siendo el mismo conjunto) tiene dos elementos. Pero esto implica que $a \neq b$. Como $\{\{a\},\{a,b\}\} = \{\{a'\},\{a',b'\}\}$, entonces $\{a\} = \{a'\}$ o $\{a\} = \{a',b'\}$. Pero la segunda opción es imposible, luego $\{a\} = \{a'\}$, es decir, $a = a'$. De manera similar, $\{a,b\} = \{a'\}$ o $\{a,b\} = \{a',b'\}$, pero la primera opción es imposible, así que $\{a,b\} = \{a',b'\}$. Esto implica que $b = a'$ o $b = b'$; sin embargo, la primera opción es imposible pues $a' = a$ y $b \neq a$. Por ende, $b = b'$.

En cualquier caso concluimos que $a = a'$ y $b = b'$. ∎

La definición de una 3-tupla es *recursiva*. Esto es, para definir una 3-tupla recurrimos a la definición de una 2-tupla: *Definición recursiva*

Definición 1.56. Dados a_1, a_2, a_3, definimos la 3-tupla (a_1,a_2,a_3) así:

$$(a_1,a_2,a_3) := ((a_1,a_2),a_3).$$

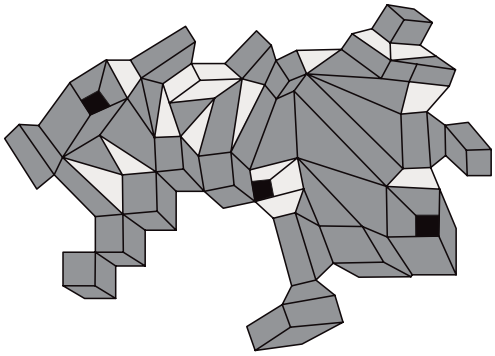
Por ejemplo, la 3-tupla (a,b,c) es igual a $((a,b),c)$, que a su vez es igual a:

$$((a,b),c) = \{\{(a,b)\},\{(a,b),c\}\} = \{\{\{\{a\},\{a,b\}\}\},\{\{\{a\},\{a,b\}\},c\}\}.$$

Como el lector se dará cuenta, toda 3-tupla es un par ordenado. En efecto, la 3-tupla (a,b,c) es el par ordenado cuyas coordenadas son (a,b) y c. De forma análoga, podemos definir una n-tupla para cualquier $n \in \mathbb{N}^*$. Para hacer esto de forma rigurosa se requiere de una definición por recursión (consulte la § 2.3 (p. 83, abajo) para más detalles).

El lector se preguntará si existen tuplas infinitas. La respuesta es que sí. Éstas se estudiarán aquí en su momento (p. 132, abajo).

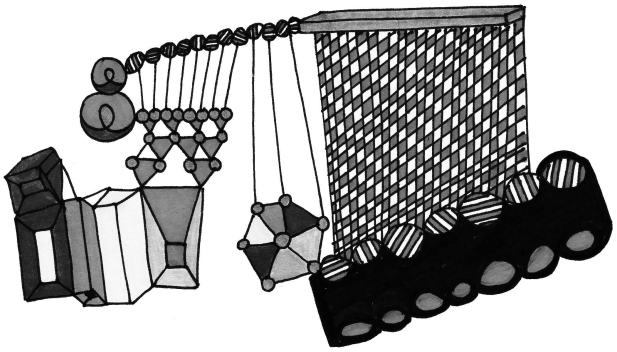
Ejercicios



1. Sea $\mathcal{U} = \{1,2,3,4,5,6,7,8,9,10\}$. Sean A, B y C los siguientes subconjuntos de $\mathcal{U}$: $A = \{1,4,5\}$, $B = \{4,6,7\}$, $C = \{2,7,8\}$.
   Calcule los siguientes conjuntos:
   (a) $A \times B$,
   (b) $A \times \varnothing$,
   (c) $A^c \times B^c$,
   (d) $\mathcal{U} \times \mathcal{U} \setminus A \times C$,
   (e) $(A \times B) \cup (A \times C)$,
   (f) $(A \cup B) \times C$,
   (g) $(A \times B) \cap (A \times C)$,
   (h) $(A \cap B) \times C$.
2. Demuestre que, dados los conjuntos A y B, $A \times \{0\} \cap B \times \{1\} = \varnothing$.
3. Demuestre que si $A \subseteq A'$ y $B \subseteq B'$ entonces $A \times B \subseteq A' \times B'$. Encuentre una condición necesaria y suficiente para que la última contenencia sea propia.
4. ¿Verdadero o falso? Si $A \times B$ y $C \times D$ no son disjuntos entonces A y C no son disjuntos y B y D no son disjuntos.
5. Demuestre el Teorema 1.53.
6. Sean $A, B, C, A', B' \subseteq \mathcal{U}$. ¿Cómo se comparan estos conjuntos?
   (a) $(A \times B) \cup (C \times D)$ vs. $(A \cup C) \times (B \cup D)$.
   (b) $(A \times B) \cap (C \times D)$ vs. $(A \cap C) \times (B \cap D)$.
   (c) $(X \setminus A) \times (Y \setminus B)$ vs. $(X \times Y) \setminus (A \times B)$.
   (d) $(\mathcal{U} \times \mathcal{U}) \setminus (A \times B)$ vs. $(A^c \times \mathcal{U}) \cup (\mathcal{U} \times B^c)$.
   (e) $\mathcal{P}(A \times B)$ vs. $\mathcal{E} = \{S \times T : (S,T) \in \mathcal{P}(A) \times \mathcal{P}(B)\}$.
   (f) $A \times (B \times C)$ vs. $(A \times B) \times C$.
7. Sean $A = \{0,1,2\}$, $B = \{1\}$ y $C = \{2,3\}$. Calcule estos conjuntos:
   (a) $(A \times B) \times C$,
   (b) $A \times (B \times C)$,
   (c) $(A \times B) \times (C \times A)$,
   (d) $C \times (C \times C)$.

8. Sean los conjuntos $S = \{(n,m) \in \mathbb{N} \times \mathbb{N} : n + m = 10\}$ y $\pi_1(S) = \{n :$ existe $m \in \mathbb{N}$ tal que $(n,m) \in S\}$. (Note que $\pi_1(S) \subseteq \mathbb{N}$.)
   (a) Demuestre que $8 \in \pi_1(S)$ y dé un ejemplo de un elemento x tal que $x \in \mathbb{N} \setminus \pi_1(S)$.
   (b) Demuestre que $\pi_1(S) = \mathbb{N}^{\leq 10}$. (Recuerde que $\mathbb{N}^{\leq 10}$ se define como $\{n \in \mathbb{N} : n \leq 10\}$.)
   (c) Demuestre que, dados los conjuntos $A, B \subseteq \mathbb{N}$, $S \neq A \times B$. (*Ayuda*: puede razonar por contradicción.)
9. Demuestre las siguientes igualdades de conjuntos:
   (a) $\bigcup_{i\in I}\bigcup_{j\in J} A_{i,j} = \bigcup_{(i,j)\in I\times J} A_{i,j}$; (b) $\bigcap_{i\in I}\bigcap_{j\in J} A_{i,j} = \bigcap_{(i,j)\in I\times J} A_{i,j}$.
10. Para todo número $a \in \mathbb{R}$, sean H_a y V_a los siguientes conjuntos:
$$H_a := \{(x,y) \in \mathbb{R}^2 : y = a\};$$
$$V_a := \{(x,y) \in \mathbb{R}^2 : x = a\}.$$
   (a) Dibuje en el plano a H_3 y V_2. Calcule el conjunto $H_3 \cap V_2$.
   (b) Dibuje en el plano el siguiente conjunto:
$$A = \left(\bigcup_{a\in[2,5]} H_a\right) \cap \left(\bigcup_{a\in[1,3]} V_a\right).$$
   (c) Dibuje en el plano el siguiente conjunto:
$$B = \left(\bigcup_{a\in[2,5]} H_a \cap V_a\right).$$
11. Dados los conjuntos A y B y $S \subseteq A \times B$, sean
$$\pi_1(S) = \{a : \exists b : (a,b) \in S\}, \quad \pi_2(S) = \{b : \exists a : (a,b) \in S\}.$$
Sea R el conjunto de los "rectángulos" de $A \times B$. Más precisamente:
$$R = \{S \times T : (S,T) \in \mathcal{P}(A) \times \mathcal{P}(B)\}.$$
Demuestre que $\pi_1(S) \times \pi_2(S)$ es el *mínimo* rectángulo que contiene a S. Esto es, que se cumplen las siguientes tres afirmaciones:
   (a) $\pi_1(S) \times \pi_2(S) \in R$;
   (b) $S \subseteq \pi_1(S) \times \pi_2(S)$;
   (c) para todo $C \in R$, si $S \subseteq C$ entonces $\pi_1(S) \times \pi_2(S) \subseteq C$.
12. Sea $Z(A,B) = \{x \in \mathcal{U} :$ Si $x \in A$ entonces $x \in B\}$ (véase el ejercicio 27 de la § 1.3). Demuestre que
$$Z(A \times B, A' \times B') = [(A \setminus A') \times B]^c \cap [A \times (B \setminus B')]^c.$$

Proyecto: Álgebras de conjuntos



En los tres ejercicios que siguen definiremos las álgebras de conjuntos y caracterizaremos algunas de ellas. Para ello fijamos cierto universo $\mathcal{U}$. Dado $A \subseteq \mathcal{U}$ definimos $A^0 := A^c$, $A^1 := A$. Sean $A_1, A_2 \subseteq \mathcal{U}$. (En los siguientes ejercicios trabajaremos con estos conjuntos; el lector podrá convencerse, que es posible generalizar los siguientes ejercicios si se consideran n conjuntos $A_1, \ldots, A_n$, o incluso un número infinito de ellos; por simplicidad, estudiaremos el caso $n = 2$.)

Problemas

1. Conjuntos básicos y estructurados:
   (a) Diremos que A es un conjunto *básico* si sucede que es de la forma $A = A_1^{i_0} \cap A_2^{i_1}$ (en donde $i_0, i_1 \in \{0, 1\}$). Demuestre que dos conjuntos básicos distintos entre sí deben ser disjuntos entre sí; en otras palabras, si A, B son básicos y $A \neq B$, entonces $A \cap B = \varnothing$.
   (b) Calcule el máximo número posible de conjuntos básicos y dé un ejemplo de este caso (debe comenzar por definir los conjuntos A_1 y A_2).
   (c) Diremos que A es un conjunto *estructurado* si A puede verse como la unión de cero o más conjuntos básicos. (En particular, el conjunto vacío es estructurado, pues es la unión de cero conjuntos básicos, y todo conjunto básico es también estructurado). Demuestre que A_1 y A_2 son conjuntos estructurados.
   (d) Calcule el máximo número posible de conjuntos estructurados, y dé un ejemplo de este caso (debe comenzar por definir los conjuntos A_1 y A_2).

2. Dado $A \subseteq \mathcal{U}$, diremos que A es un conjunto *completo* si para toda elección de $i_1, i_2 \in \{0,1\}$, se tiene que

$$\text{si } A \cap A_1^{i_1} \cap A_2^{i_2} \neq \varnothing, \text{ entonces } A \supseteq A_1^{i_1} \cap A_2^{i_2}.$$

Demuestre las siguientes afirmaciones:

   (a) A_1 y A_2 son conjuntos completos.

   (b) Si A y B son conjuntos completos, entonces $A \cap B$ es un conjunto completo.

   (c) Si A es un conjunto completo, entonces A^c es un conjunto completo.

   (d) Si A y B son conjuntos completos, entonces $A \cup B$ es un conjunto completo. (*Ayuda*: suponga que A y B son completos, y utilice los sub-ejercicios anteriores, junto con el hecho de que $A \cup B = (A^c \cap B^c)^c$.)

   (e) Todo conjunto básico es completo.

   (f) Para todo A, A es completo si y sólo si A es estructurado.

3. Dado $\mathcal{C} \subseteq \mathcal{P}(\mathcal{U})$, diremos que $\mathcal{C}$ es un *álgebra de conjuntos* si $\mathcal{C}$ es cerrado bajo unión, intersección y complemento. En otras palabras, si para todo $A, B \subseteq \mathcal{U}$ se tiene:

$$\text{Si } A, B \in \mathcal{C}, \text{ entonces } A \cup B \in \mathcal{C}, A \cap B \in \mathcal{C} \text{ y } A^c \in \mathcal{C}.$$

   (a) Demuestre que si $\mathcal{C}$ es un álgebra de conjuntos y $\mathcal{C} \neq \varnothing$, entonces $\varnothing \in \mathcal{C}$ y $\mathcal{U} \in \mathcal{C}$.

   (b) Demuestre que si $\mathcal{C}$ y $\mathcal{D}$ son álgebras de conjuntos, entonces $\mathcal{E} := \mathcal{C} \cap \mathcal{D}$ es también un álgebra de conjuntos.

   (c) Sea $\mathcal{C}_0 := \{A \in \mathcal{P}(\mathcal{U}) : A \text{ es un conjunto completo}\}$. Demuestre que $\mathcal{C}_0$ es un álgebra de conjuntos.

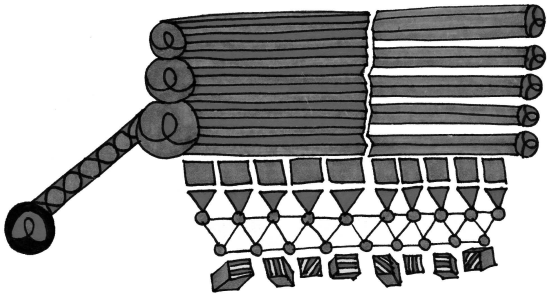
   (d) Demuestre que si $\mathcal{C}$ es un álgebra de conjuntos tal que $A_0 \in \mathcal{C}$ y $A_1 \in \mathcal{C}$, entonces $\mathcal{C}_0 \subseteq \mathcal{C}$. (*Ayuda*: si $A \in \mathcal{C}_0$, entonces A es completo, luego A es estructurado. Demuestre ahora que $\mathcal{C}$ debe tener como elemento a todo conjunto básico (dado que tiene a A_0 y A_1 como elementos) y, por ende, a todo conjunto estructurado, de modo que $A \in \mathcal{C}$.)

   (e) Por lo anterior, $\mathcal{C}_0$ es la *mínima álgebra de conjuntos que tiene a A_0 y a A_1 como elementos*. Demuestre que

$$\mathcal{C}_0 = \bigcap \{\mathcal{C} : \mathcal{C} \text{ es un álgebra de conjuntos y } A_0, A_1 \in \mathcal{C}\}.$$

   En particular, un conjunto A es completo (o estructurado) si y sólo si A pertenece a *todas* las álgebras de conjuntos $\mathcal{C}$ tales que A_0 y A_1 pertenecen a $\mathcal{C}$.

Lecturas adicionales



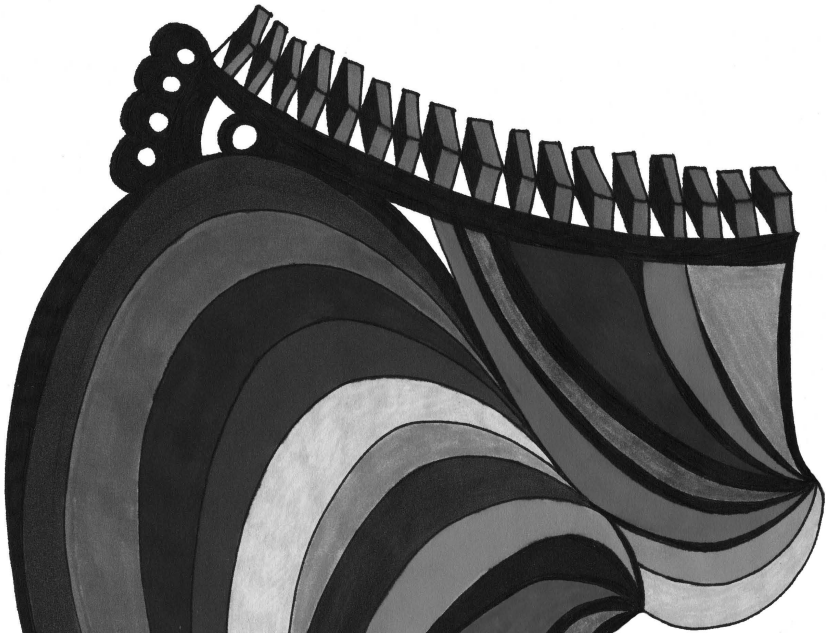
Se recomienda consultar las siguientes lecturas, con miras a profundizar en algunos de los temas tratados en este capítulo:[14]

- Para más información sobre teoría de conjuntos, consulte [8], §§ 1.1–1.5; [2], §§ 1.1–1.3; [4], c. 1; [6], § 2.1; [11], §§ 8–10.
- Para más información sobre órdenes parciales, consulte [11], § 50.
- Para una exposición axiomática de la teoría de conjuntos, consulte [4], § 1.3; [2], § 6.1.

[14] Para la bibliografía, cf. p. 313, abajo.

CAPÍTULO 2

INDUCCIÓN: LOS NÚMEROS NATURALES



Estructuras ordenadas...

En este capítulo haremos un estudio detallado de la estructura de orden del conjunto de los números naturales, la cual tiene varias propiedades que permiten analizar a cada número natural n distinto de 0 en términos de su predecesor inmediato; introduciremos un método de demostración llamado *inducción*, utilizado para demostrar que cierta propiedad p es válida para todos los números naturales. Informalmente este método es llamado así, pues el hecho de que cualquier número natural n tenga la propiedad induce a que su sucesor inmediato, $n+1$, también la tenga.

Más adelante veremos aplicaciones de la inducción: estudiaremos la definición de funciones mediante recursión y estableceremos algunos

métodos básicos de conteo finito. También estudiaremos más a fondo la noción de estructura ordenada, introduciendo para ello el concepto de isomorfismo.

§ 2.1 El Principio del Buen Orden

Comencemos redondeando algunas ideas acerca de los conjuntos ordenados que mencionamos anteriormente (cf. § 1.2, pp. 15 ss).

Definición 2.1 (Orden parcial). Una *estructura parcialmente ordenada* $(A, \leq)$ consiste en un conjunto no vacío A y una relación $\leq$ sobre A que cumple con las siguientes tres propiedades:

(a) *Reflexividad*: $\forall x \in A : x \leq x$ (todo elemento en A se relaciona consigo mismo).

(b) *Antisimetría*: $\forall x, y \in A : (x \leq y \wedge y \leq x) \to x = y$ (dados $x, y \in A$, si x se relaciona con y y y se relaciona con x, entonces $x = y$).

(c) *Transitividad*: $\forall x, y, z \in A : (x \leq y \wedge y \leq z) \to x \leq z$ (dados $x, y, z \in A$, si x se relaciona con y y y se relaciona con z, entonces x se relaciona con z).

Orden parcial

Bajo estas condiciones diremos que $\leq$ es un *orden parcial* sobre A.

Definición 2.2 (Orden lineal). Una *estructura linealmente ordenada* o *totalmente ordenada* $(A, \leq)$ consiste en un conjunto A y un orden parcial $\leq$ sobre A, que asimismo cumple la siguiente condición llamada *comparabilidad*:

Comparabilidad

$$\text{Si } a, b \in A, \text{ entonces } a \leq b \text{ o } b \leq a.$$

Orden lineal

Bajo estas condiciones diremos que $\leq$ es un *orden lineal* (o *total*) sobre A. También se dice que $\leq$ *ordena linealmente* a A. Por convención, $a < b$ significa: $a \leq b$ y $a \neq b$.

Definición 2.3 (Elemento mínimo). Sea $(A, \leq)$ una estructura parcialmente ordenada y sea $B \subseteq A$. Dado $m \in A$, se dice que m es un *elemento mínimo de* B (y escribimos $m = \min(B)$) si se cumple:

$\min(B)$: *Mínimo de B*

$$m \in B \text{ y } \forall x \in B : m \leq x.$$

En este capítulo estudiaremos principalmente órdenes lineales. Un ejemplo importante de ellos es la estructura ordenada de los números enteros, la cual tiene como conjunto base el de los números enteros:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

El orden $\leq$ que consideramos sobre $\mathbb{Z}$ es el tradicional; por ejemplo, $2 \leq 5$ (el 2 está "por debajo" del 5), $-1 \leq 0$, $-4 \leq -3$, $3 \leq 3$, etc. Puede verificarse que este orden es lineal. Informalmente, este orden es similar a un pozo sin fondo, puesto que —por ejemplo— por debajo del 4 podemos encontrar *infinitos* números enteros $(3, 2, 1, 0, -1, -2, \dots)$, sin llegar así a un mínimo o tocar fondo, de acuerdo con la analogía del pozo. En este sentido podríamos decir informalmente que $\mathbb{Z}$ es un conjunto *mal ordenado*.

Veamos otro ejemplo un poco más interesante. Consideremos el conjunto de todos los números reales positivos junto con el 0, con su orden lineal usual:

$$A = \{r \in \mathbb{R} : r \geq 0\} = [0, \infty).$$

En este orden, por ejemplo, $0 \leq 2/3 \leq \sqrt{2} \leq 2 \leq \pi \leq 1000$, y claramente el 0 es el mínimo elemento de A. Sea S el siguiente subconjunto de A:

$$S = (1, 2) = \{r \in \mathbb{R} : 1 < r < 2\}.$$

Es claro que $S \subseteq A$ y, además, que S no tiene un elemento mínimo: dado $r \in S$, se tiene que $1 < r$. Luego siempre es posible encontrar un número s entre 1 y r, esto es, un número tal que

$$1 < s < r.$$

Por ejemplo, tomamos a s como el promedio entre 1 y r; en otras palabras, $s = (r + 1)/2$. S es un subconjunto no vacío de A que no tiene un elemento mínimo; en este sentido podemos decir informalmente que A se encuentra "mal ordenado", pues algunas de sus regiones (es decir, algunos de sus subconjuntos no vacíos) son pozos sin fondo, esto es, no tienen elementos mínimos.

La discusión anterior da pie a la siguiente definición:

Definición 2.4 (Buen orden). Sea $(A, \leq)$ una estructura linealmente ordenada. Diremos que $(A, \leq)$ es un *buen orden* (o A es un conjunto bien ordenado por $\leq$) si todo subconjunto no vacío de A tiene un elemento mínimo m. En términos formales, si se cumple:

Buen orden

$$\forall S \subseteq A : (S \neq \varnothing \to \exists m \in S : (\forall x \in S : m \leq x)).$$

Como explicamos en el ejemplo anterior, el conjunto de los números reales mayores o iguales que 0, con su orden usual, no es un conjunto bien ordenado. En cambio, resulta que $(\mathbb{N}, \leq)$ sí lo es y este hecho se conoce como el *Principio del Buen Orden* (PBO). Intuitivamente esto lo justificamos así: si A es un subconjunto no vacío de números naturales, entonces debe tener un elemento $a_0 \in S$. Si éste no es el elemento mínimo en S, es por que existe $a_1 \in S$, $a_1 < a_0$. Si a_1 es el elemento mínimo en S, lo hemos encontrado y si no, es por que existe $a_2 < a_1$, $a_2 \in S$. Pero este

PBO: *Principio del Buen Orden*

proceso de búsqueda del mínimo lo podemos repetir tan sólo un número finito de veces, pues sólo hay un número finito de números naturales debajo de a_0. Cuando ya no podamos seguir con el procedimiento anterior, el último elemento que hayamos encontrado en S tendrá que ser su elemento mínimo.

Principio 2.5 (Principio del Buen Orden, PBO). La estructura $(\mathbb{N}, \leq)$ es un buen orden.

☞ **Antes de seguir leyendo**

1. ¿Verdadero o falso? Si $(A, \leq)$ es un buen orden, entonces A tiene un elemento mínimo.
2. Demuestre que si $\leq$ es un orden parcial sobre A, $S \subseteq A$ y $m, m' \in S$ verifican que $\forall x \in S : m \leq x$ y $\forall x \in S : m' \leq x$, entonces $m = m'$. (Esto demuestra que en órdenes parciales el elemento mínimo de un conjunto, en caso de existir, es único.)
3. ¿Cuáles de las siguientes estructuras son buenos órdenes?
   (a) $(\mathbb{Q}, \leq)$,
   (b) $(\mathbb{Q}^{\geq 0} = \{q \in \mathbb{Q} : q \geq 0\}, \leq)$,
   (c) $(P = \{n \in \mathbb{N} : n \text{ es primo }\}, \leq)$,
   (d) $(\mathbb{Z}, \leq)$,
   (e) $(\{1, 2, 3\}, \leq)$,
   (f) $(\{n + \frac{1}{m+1} : n, m \in \mathbb{N}\}, \leq)$,
   (g) $(\mathbb{Z}^-, \leq)$,
   (h) $(\mathcal{P}(\mathbb{N}), \subseteq)$.
4. Sea A el conjunto $A = \mathbb{N} \times \{0, 1\}$, y defina un orden sobre A de la siguiente manera: dados $(a, i), (b, j) \in A$:
   (i) si $i < j$, entonces $(a, i) \leq (b, j)$;
   (ii) si $i = j$ y $a \leq b$, entonces $(a, i) \leq (b, j)$.
   Por ejemplo, $(5, 0) \leq (2, 1)$ y $(8, 0) \leq (9, 0)$. Demuestre que la estructura $(A, \leq)$ es un buen orden.

El buen orden de la estructura $(\mathbb{N}, \leq)$ permite demostrar ciertas propiedades que valen para todo número natural:

Ejemplo 2.6. Demuestre que para todo $n \in \mathbb{N}$,

$$0 + 1 + \cdots + n = n(n+1)/2.$$

Solución. Dado $n \in \mathbb{N}$, sea $p(n)$ la afirmación $0+1+\cdots+n = n(n+1)/2$. $p(n)$ es una afirmación que puede ser verdadera o falsa, según el valor de n. Por ejemplo, como $0+1+2+3 = 6 = 3(4)/2$, entonces $p(3)$ es una afirmación verdadera. Ahora, sea

$$A = \{n \in \mathbb{N} : p(n)\},$$

esto es, A es el conjunto de números naturales que tienen la propiedad p. Como $0 = 0(1)/2$, concluimos que $p(0)$ es verdadera, esto es, $0 \in A$. Queremos ver que

$$\forall n \in \mathbb{N} : 0 + \cdots + n = n(n+1)/2,$$

o en otras palabras, que $A = \mathbb{N}$.

Razonamos por contradicción: si $A \neq \mathbb{N}$, entonces $A^c = \mathbb{N} \setminus A$ es un subconjunto *no vacío* de $\mathbb{N}$. Por el PBO, este subconjunto debe tener un elemento mínimo $m \in A^c$. Pero $0 \in A$, así que $m \neq 0$. Esto implica que existe $n \in \mathbb{N}$ tal que $m = n + 1$.[1] Como $n < m$ y m es el elemento mínimo de A^c, concluimos que $n \in A$, es decir, $p(n)$ es válida:

$$0 + \cdots + n = n(n+1)/2.$$

Ahora, si sumamos $n+1$ a ambos lados de la ecuación anterior obtenemos:

$$\begin{aligned} 0 + 1 + \cdots + n + (n+1) &= n(n+1)/2 + (n+1) \\ &= (n^2 + n + 2n + 2)/2 \\ &= (n+1)(n+2)/2 \\ &= (n+1)((n+1)+1)/2 \\ &= m(m+1)/2. \end{aligned}$$

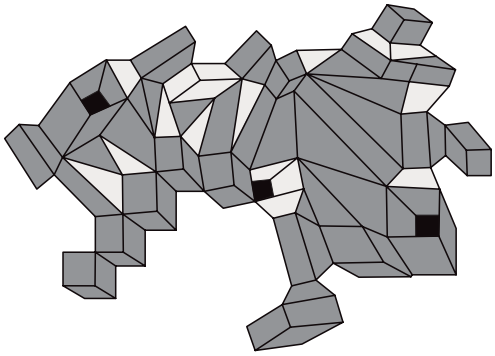
Concluimos que

$$0 + \cdots + (n+1) = 0 + \cdots + m = m(m+1)/2,$$

lo cual significa que $p(m)$ es verdadera, esto es, $m \in A$. Esto contradice el hecho de que $m \in A^c$. Se sigue que $A^c = \varnothing$, luego $A = \mathbb{N}$, como queríamos demostrar. ∎

[1] Véase la Observación 2.7 (b), abajo.

Ejercicios



1. Para cada una de las siguientes propiedades p, determine el mínimo número natural n_0, si es que existe, tal que la propiedad evaluada en n es verdadera, para todo $n \in \mathbb{N}$ tal que $n \geq n_0$:
   (a) $p(n)$: "$2n > 7$".
   (b) $p(n)$: "Si $n > 3$, entonces $n > 2$".
   (c) $p(n)$: "$n^2 \leq 100$".
   (d) $p(n)$: "$n^2 - n \geq n$".
   (e) $p(n)$: "Todo conjunto con n elementos tiene siempre más de n subconjuntos".
   (f) $p(n)$: "$2 + 2 = 4$".
2. Si $(A, \leq)$ es un buen orden, y $B \subseteq A$, ¿es necesariamente $(B, \leq)$ un buen orden? Explique su respuesta.
3. Sea $A \subseteq \mathbb{R}$.
   (a) Si A es un buen orden, ¿necesariamente A tiene un elemento mínimo? ¿Por qué?
   (b) Si A tiene un elemento mínimo, ¿necesariamente A es un buen orden? ¿Por qué?
   (c) Encuentre un conjunto $B \subseteq [0,1]$ tal que B sea un buen orden infinito.
4. Dado un orden lineal $O = (A, \leq)$, defina el orden inverso de O como el orden $(A, \leq^{-1})$, en donde dados $a, b \in A$, $a \leq^{-1} b$ si y sólo si $b \leq a$. Demuestre las siguientes afirmaciones:
   (a) $(\mathbb{N}, \leq^{-1})$ no es un buen orden.
   (b) $(\mathbb{Z}^-, \leq^{-1})$ es un buen orden.

5. Utilice el PBO para demostrar que, si $\varnothing \subset A \subseteq \mathbb{Z}$ y A está acotado superiormente (esto es, existe $c \in \mathbb{Z}$ tal que para todo $a \in A$ $a \leq c$), entonces A tiene un elemento máximo.

§ 2.2 Demostraciones por inducción

A continuación enunciamos algunas propiedades fundamentales de la estructura $(\mathbb{N}, \leq)$. El lector interesado en demostrarlas a partir de la definición precisa de $(\mathbb{N}, \leq)$ puede referirse a los ejercicios 15 y posteriores de esta sección.

Observación 2.7. La estructura $(\mathbb{N}, \leq)$ cumple con las siguientes propiedades:

(a) $\leq$ es un orden parcial sobre $\mathbb{N}$.
(b) $0 \in \mathbb{N}$ es el elemento mínimo de $\mathbb{N}$.
(c) Para todo $n \in \mathbb{N}$, $n < n+1$ y no existe $m \in \mathbb{N}$ tal que $n < m < n+1$.
(d) Para todo $n \in \mathbb{N}$, si $n \neq 0$, entonces existe $m \in \mathbb{N}$ tal que $m + 1 = n$.

En esta sección presentaremos dos principios equivalentes al PBO. Para esto necesitamos definir primero la noción de *conjunto inductivo*:

Definición 2.8 (Conjunto inductivo). Dado un $A \subseteq \mathbb{N}$, diremos que A es un *conjunto inductivo* si para todo $n \in A$, $n + 1 \in A$.

Conjunto inductivo

Por ejemplo, el conjunto vacío y el conjunto de los números naturales son conjuntos inductivos, mientras que el conjunto de los números pares no lo es. El conjunto de los números naturales menores que 300 no es inductivo, pero su complemento sí lo es.

Como el lector se habrá dado cuenta en la solución del ejemplo 2.6, los dos hechos claves para demostrar que $A = \mathbb{N}$ fueron, en primer lugar, que $0 \in A$; en segundo lugar, que para todo n, $p(n) \to p(n+1)$, es decir, si $n \in A$ entonces $n + 1 \in A$ o, en otras palabras, A es un conjunto inductivo. El siguiente principio, llamado el *Principio de Inducción*, establece que este razonamiento es válido en general:

Principio 2.9 (Principio de Inducción, PI). Sea A un subconjunto de $\mathbb{N}$ tal que $0 \in A$ y A es un conjunto inductivo. Entonces $A = \mathbb{N}$.

PI: *Principio de Inducción*

Es fácil convencerse de la validez de este principio: si $0 \in A$ y A es inductivo, entonces $1 \in A$, pero entonces $2 \in A$, pero entonces..., pero

entonces $n \in A$, pero entonces $n+1 \in A$... Como este razonamiento continúa indefinidamente, en A podremos "capturar" a todos los números naturales y así $\mathbb{N} \subseteq A$. Por otro lado, A es un subconjunto de $\mathbb{N}$, por el PE concluimos que $A = \mathbb{N}$. (Para una demostración rigurosa del PI, véanse los ejercicios 13 y 14.)

Lema 2.10 (Caso base, paso inductivo). El PI es equivalente a la siguiente afirmación: si p es una propiedad cualquiera relativa a los números naturales, tal que

(a) $p(0)$, esto es, 0 tiene la propiedad p, y

(b) p es una propiedad inductiva en el siguiente sentido: para todo número natural n, si $p(n)$, entonces $p(n+1)$, es decir, el hecho de que n tenga la propiedad p induce que su sucesor inmediato $n+1$ también la tenga,

entonces, todos los números naturales tienen la propiedad p o, más formalmente, $\forall n \in \mathbb{N} : p(n)$.

Prueba. Demostremos primero que el PI implica la afirmación anterior. Para esto supongamos que $p(0)$ y que para todo $n \in \mathbb{N}$, $p(n) \to p(n+1)$. Queremos demostrar lo siguiente: $\forall n \in \mathbb{N} : p(n)$. Sea A el subconjunto de $\mathbb{N}$ definido así: $A = \{n \in \mathbb{N} : p(n)\}$. Por hipótesis, $0 \in A$, ya que $p(0)$, y, además, A es un conjunto inductivo, puesto que para todo $n \in \mathbb{N}$, $n \in A$ implica $p(n)$ y esto implica $p(n+1)$ y, por lo tanto, $n+1 \in A$, donde la segunda implicación vale por hipótesis. Por el PI, $A = \mathbb{N}$, lo cual garantiza que $\forall n \in \mathbb{N} : n \in A$, es decir, $\forall n \in \mathbb{N} : p(n)$.

Ahora supongamos que la afirmación del lema es válida y demostremos que el PI es válido. Sea A un subconjunto inductivo de $\mathbb{N}$, tal que $0 \in A$. Queremos demostrar que $A = \mathbb{N}$. Definimos p como la propiedad "pertenecer a A", esto es, $p(n)$ es la afirmación "$n \in A$". Como $0 \in A$, entonces $p(0)$ y como A es inductivo, podemos afirmar que $\forall n \in \mathbb{N} : p(n) \to p(n+1)$. Por hipótesis, concluimos que todo número natural tiene la propiedad p, esto es, $\mathbb{N} \subseteq A$. Como A es un subconjunto de $\mathbb{N}$, concluimos que $A = \mathbb{N}$. ∎

Por el lema anterior, para demostrar que todos los números naturales tienen cierta propiedad p, basta demostrar dos afirmaciones:

(a) Caso base ($n = 0$): 0 tiene la propiedad p.

(b) Paso inductivo: para todo número natural n, si n tiene la propiedad p, entonces $n+1$ también la tiene.

Demostración por inducción

El anterior esquema corresponde a una *demostración por inducción*. Una demostración por inducción de que todos los números naturales

tienen cierta propiedad p consiste en realidad en dos demostraciones: el caso base y el paso inductivo. Éstas deben hacerse por separado y, por supuesto, no bastará en general con demostrar el paso inductivo. Por ejemplo, una prueba (incorrecta) de que todo número natural es mayor que 5 sería la siguiente:

> Supongamos que $n > 5$. Entonces, si sumamos 1 a ambos lados de la ecuación, obtenemos que $n + 1 > 5 + 1 > 5$, luego $n + 1 > 5$. Por el PI (PI), concluimos que todo número natural es mayor que 5.

En la anterior "demostración" hizo falta el caso base, que es por supuesto falso, pues 0 no es mayor que 5.

Ejemplo 2.11. Demuestre por inducción que, para todo $n \in \mathbb{N}$,

$$0 + 1 + \cdots + n = n(n+1)/2.$$

Solución. Demostramos la propiedad en cuestión mediante el PI:

(a) Caso base ($n = 0$): como $0 = 0(1)/2$, concluimos que la afirmación es verdadera cuando $n = 0$.

(b) Paso inductivo: sean $n \in \mathbb{N}$ y supongamos que la propiedad en cuestión vale para n, es decir, que

$$0 + 1 + \cdots + n = n(n+1)/2. \qquad \text{(Hip. de inducción)}$$

Queremos demostrar que la propiedad vale para $n+1$, es decir, queremos ver que

$$0 + 1 + \cdots + n + (n+1) = (n+1)[(n+1)+1]/2.$$

Si partimos de la hipótesis de inducción y sumamos $n + 1$ a ambos lados de esta ecuación, obtenemos:

$$\begin{aligned} 0 + 1 + \cdots + n + (n+1) &= n(n+1)/2 + (n+1) \\ &= (n^2 + n + 2n + 2)/2 \\ &= (n+1)(n+2)/2 \\ &= (n+1)[(n+1)+1]/2. \end{aligned}$$

Concluimos que la propiedad vale para $n + 1$.

Por el PI, todo número natural cumple la propiedad, es decir, para todo $n \in \mathbb{N}$, $0 + 1 + \cdots + n = n(n+1)/2$. ∎

Ejemplo 2.12. Demuestre por inducción que para todo $n \in \mathbb{N}$ se tiene que $n(n+1)$ es par, esto es, es divisible por 2.

Solución. En general, un número entero n es divisible por 2 si existe un número entero k tal que $n = 2k$. Así, debemos demostrar que $n(n+1)$ es siempre de la forma $2k$ para algún entero k. Lo hacemos mediante inducción:

(a) Caso base ($n = 0$): $0(1) = 0 = 2(0)$ y, por lo tanto, es par.

(b) Paso inductivo: supongamos que la propiedad en cuestión vale para n, es decir, que $n(n+1)$ es divisible por 2. En otras palabras, supongamos que

$$\exists k \in \mathbb{Z} : n(n+1) = 2k. \qquad \text{(Hip. de inducción)}$$

Queremos demostrar que la propiedad vale para $n+1$, es decir, queremos ver que $(n+1)[(n+1)+1]$ también es de la forma $2m$ para algún número entero m. Tenemos:

$$\begin{aligned}(n+1)[(n+1)+1] &= (n+1)(n+2)\\ &= n(n+1) + 2(n+1)\\ &= 2k + 2(n+1) \qquad \text{(Hip. de inducción)}\\ &= 2(k+n+1).\end{aligned}$$

Como $m := k+n+1$ es un número entero (pues k, n y 1 lo son), concluimos que $(n+1)[(n+1)+1]$ es divisible por 2, como se quería.

Por el PI, todo número natural cumple la propiedad, es decir, para todo $n \in \mathbb{N}$, $n(n+1)$ es par. ■

Ahora veamos otro principio de inducción, llamado el *Principio de Inducción Fuerte*, el cual es equivalente al PI, como veremos más adelante.

PIF: *Principio de Inducción Fuerte*

Principio 2.13 (Principio de Inducción Fuerte, PIF). Sea $A \subseteq \mathbb{N}$ tal que para todo número natural n vale lo siguiente:

$$(\forall k \in \mathbb{N} : k < n \to k \in A) \to n \in A.$$

Entonces $A = \mathbb{N}$.

En el PI, utilizado como un método de demostración, la hipótesis de inducción es $p(n-1)$, a partir de la cual se deberá demostrar $p(n)$. Ahora bien, en el PIF, utilizado como un método de demostración, la hipótesis de inducción es "$p(0)$ y $p(1)$ y ... y $p(n-1)$", a partir de la cual se deberá demostrar $p(n)$. Veamos un ejemplo:

Ejemplo 2.14. Suponiendo el PIF, demuestre que para todo $n \in \mathbb{N}$ se tiene que n es divisible por 3 si y sólo si la suma de los dígitos de n es divisible por 3.

Solución. Sea A el conjunto de los números naturales que cumplen con tal propiedad. Debemos demostrar que para todo $n \in \mathbb{N}$ vale lo siguiente:

si para todo $k < n$, k tiene la propiedad,
entonces n tiene la propiedad.

Los casos en los cuales $n = 0, 1$ y 2 son fáciles de verificar y se dejan al lector. Supongamos entonces que $n \in \mathbb{N}$ y $n > 2$, y supongamos que todo $k \in \mathbb{N}$ con $k < n$ tiene la propiedad. Demostremos que n tiene la propiedad. Para ello, dado cualquier número entero k, sea s_k la suma de todos los dígitos de k. Utilizamos el método de doble implicación:

($\rightarrow$) Supongamos que n es divisible por 3: entonces existe $m \in \mathbb{N}$ tal que $n = 3m$. Sea $k := n - 3 = 3(m-1)$. Tenemos que k es un número natural divisible por 3 y menor que n, luego por hipótesis de inducción se tiene que la suma de los dígitos de k, s_k es divisible por 3, es decir, existe $\alpha \in \mathbb{Z}$ tal que $s_k = 3\alpha$. Hay 3 casos:

(i) k termina en $0, 1, 2, 3, 4, 5$ o 6: en este caso es fácil ver que $s_n = s_k + 3$ y así $s_n = 3(\alpha + 1)$, luego s_n es divisible por 3.

(ii) k termina en 7: entonces podemos describir los dígitos de k como sigue:

- los primeros dígitos de k son números del 1 al 9, y el último dígito de estos k dígitos, a_p, es distinto de 9;
- los siguientes dígitos de k son todos 9, digamos que hay r de ellos, en donde r puede ser 0; y
- el último dígito de k es igual a 7.

Esto es, k tiene como dígitos:

$$a_0 a_1 \cdots a_p \underbrace{99\cdots9}_{r \text{ veces}}7,$$

lo cual implica que n tiene como dígitos

$$a_0 a_1 \cdots (a_p + 1) \underbrace{00\cdots00}_{r \text{ veces}},$$

por lo cual

$$s_n = s_k + 1 - 9r - 7 = s_k - 9r - 6 = 3(\alpha - 3r - 2).$$

Esto implica que s_n es divisible por 3.

(iii) k termina en 8 o 9: el razonamiento es análogo al anterior.

($\leftarrow$) Supongamos que s_n es divisible por 3: entonces existe $\alpha \in \mathbb{Z}$ tal que $s_n = 3\alpha$. Sea $k = n - 3$. Hay 3 casos:

(i) n termina en $3, 4, 5, 6, 7, 8$ o 9: en este caso es fácil ver que $s_k = s_n - 3$. Por ende, $s_k = 3(\alpha - 1)$, luego s_k es divisible por 3. Como $k < n$, esto implica por hipótesis de inducción que k es divisible por 3, luego existe $\beta \in \mathbb{Z}$ tal que $k = 3\beta$. Entonces

$$n = k + 3 = 3(\beta + 1),$$

luego n es divisible por 3.

(ii) n termina en 0: entonces k termina en 7 y podemos describir los dígitos de k como sigue:

- los primeros dígitos de k son números del 1 al 9 y el último dígito de ellos, a, es distinto de 9;
- los siguientes dígitos de k son todos 9, digamos que hay r de ellos, en donde r puede ser 0; y
- el último dígito de k es un 7.

Esto es, k tiene como dígitos:

$$a_0 a_1 \cdots a_p \underbrace{99\cdots97}_{r \text{ veces}},$$

lo cual implica que n tiene como dígitos

$$a_0 a_1 \cdots (a_p + 1) \underbrace{00\cdots00}_{r \text{ veces}},$$

y por ende,

$$s_n = s_k + 1 - 9r - 7 = s_k - 9r - 6.$$

Entonces

$$s_k = s_n + 9r + 6 = 3(\alpha + 3r + 2),$$

luego s_k es divisible por 3. Como $k < n$, esto implica por hipótesis de inducción que k es divisible por 3, luego existe $\beta \in \mathbb{Z}$ tal que $k = 3\beta$. Entonces $n = k + 3 = 3(\beta + 1)$, luego n es divisible por 3.

(ii) n termina en 1 o 2: el razonamiento es análogo al anterior. ■

El PI permite concluir que un conjunto $A \subseteq \mathbb{N}$ es igual a $\mathbb{N}$ a partir de dos condiciones: tener a 0 como elemento y ser un conjunto inductivo. En cambio, en el PIF sólo se requiere una condición, aunque más compleja: que para todo $n \in \mathbb{N}$, si todos los números naturales menores que n pertenecen a A, entonces n también pertenece a A.

Si bien no hemos dado una demostración de que $(\mathbb{N}, \leq)$ es un buen orden, ni hemos probado los dos principios de inducción que hemos formulado, es el caso, sin embargo, que estas tres propiedades son equivalentes entre sí. En otras palabras, si una de ellas es verdadera, las otras dos también lo son:

Teorema 2.15. Los siguientes principios son equivalentes entre sí:

(a) PBO, (b) PI, (c) PIF.

Prueba. Demostraremos por separado las siguientes implicaciones que (a) → (b), (b) → (c) y (c) → (a). Esto será suficiente para concluir que (a), (b) y (c) son equivalentes entre sí.

(a) → (b) Supongamos que $(\mathbb{N}, \leq)$ es un buen orden y demostremos el PI: sea $A \subseteq \mathbb{N}$ tal que $0 \in A$ y A es inductivo. Queremos concluir que A consta de todos los números naturales. Razonamos por contradicción. Si esto no es así, entonces el conjunto $A^c = \mathbb{N} \setminus A$ es no vacío. Luego, por hipótesis, A^c tiene un elemento mínimo, digamos $m \in A^c$. Como $0 \in A$, necesariamente $m \neq 0$. Por lo tanto, m es de la forma $n + 1$ para algún natural n. Resumiendo, tenemos lo siguiente:

$$n < n + 1 = m \in A^c.$$

Como m es el elemento mínimo de A^c, necesariamente $n \notin A^c$, es decir, $n \in A$. Como A es inductivo, $n + 1 \in A$. Pero $n + 1 = m \in A^c$. Esto es una contradicción, pues ningún elemento puede pertenecer a un conjunto y a su complemento. Esto demuestra que A^c es vacío, es decir que $A = \mathbb{N}$, como se quería.

(b) → (c) Supongamos que el PI es válido y demostremos el PIF. Sea $A \subseteq \mathbb{N}$ un conjunto tal que para todo número natural n vale lo siguiente:

$$(\forall k \in \mathbb{N} : k < n \to k \in A) \to n \in A. \qquad (*)$$

Debemos concluir que $A = \mathbb{N}$. Sea $\hat{A} = \{n \in \mathbb{N} : 0, \ldots, n \in A\}$. En otras palabras, $n \in \hat{A}$ si y sólo si el conjunto $\{0, \ldots, n\}$ está contenido en A. Note que para $n = 0$ vale trivialmente que todo número natural k menor que 0 pertenece a A. La razón es que si esto fuera falso, entonces existiría un número natural k menor que 0 que no pertenece a A, pero sencillamente no existen naturales menores que 0. Por lo tanto, formalmente vale lo siguiente:

$$(\forall k \in \mathbb{N} : k < 0 \to k \in A).$$

Por $(*)$, concluimos que $0 \in A$, es decir, $\{0\} \subseteq A$ y por ende, $0 \in \hat{A}$. Ahora probemos que $\hat{A}$ es un conjunto inductivo: sea n un número natural tal que $n \in \hat{A}$. Entonces $0, \ldots, n \in A$. Por $(*)$, esto implica que $n + 1 \in A$ y así:

$$0, \ldots, n, n + 1 \in A,$$

es decir, $n + 1 \in \hat{A}$. Como $\hat{A}$ es un conjunto inductivo que contiene al 0, concluimos, mediante el PI, que $\hat{A} = \mathbb{N}$. Pero $\hat{A} \subseteq A$ (véase el ejercicio 1), luego $\mathbb{N} \subseteq A$. Como ya teníamos la otra inclusión, concluimos la igualdad, esto es, que $A = \mathbb{N}$. Esto demuestra el PIF.

(c) → (a) Supongamos que el PIF es válido y demostremos el PBO. Observemos que para cualquier conjunto $A \subseteq \mathbb{N}$ ocurre alguno de los siguientes dos casos:

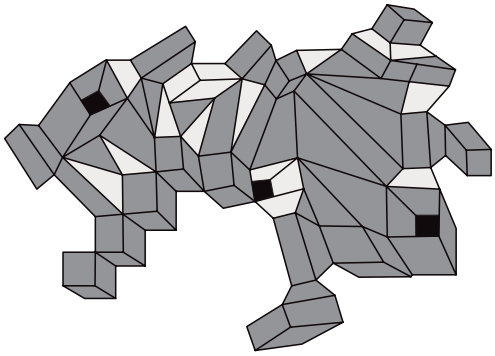
(i) Existe $n \in \mathbb{N}$ tal que para todo $k < n$, $k \in A^c$ y, además, $n \in A$. Esto significa que todo elemento menor que n no pertenece a A, luego n es el mínimo de A.

(ii) No se da el caso (i): es decir, para todo $n \in \mathbb{N}$, si para todo $k < n$ tenemos que $k \in A^c$, entonces $n \in A^c$. En este caso podemos utilizar directamente el PIF para concluir que $A^c = \mathbb{N}$, lo cual implica que $A = \varnothing$.

Si A no es vacío, el caso (ii) no puede ocurrir, luego necesariamente A debe tener un elemento mínimo. ∎

Hemos afirmado atrás que el PI es verdadero; por el teorema anterior, también serán verdaderos el PIF y el PBO.

Ejercicios



1. Dado un conjunto $A \subseteq \mathbb{N}$, sea $\hat{A} = \{n \in \mathbb{N} : 0, \ldots, n \in A\}$.
   (a) Demuestre que $\hat{A} \subseteq A$.
   (b) Demuestre que si $\hat{A}$ es no vacío y no tiene elemento máximo, entonces $A = \mathbb{N}$.
   (c) Si $A = \{2n : n \in \mathbb{N}\}$, calcule $\hat{A}$.
2. Demuestre por inducción que para todo número natural n, se cumplen las siguientes afirmaciones:
   (a) Si $n > 0$, entonces $1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$.
   (b) Si $n > 0$, entonces $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.
   (c) Si $n \geq 2$ entonces $n^2 \geq n + 1$.
   (d) Si $n \geq 4$ entonces $n^2 \leq n!$.
   (e) 5^{n+1} tiene un 5 como último dígito.
   (f) $1 + nh \leq (1 + h)^n$, con $h \in \mathbb{R}, -1 < h$.
   (g) Si $n > 1$, $n! < n^n$.
   (h) $n^2 \leq 3^n$.
   (i) Si $n > 1$, $|x_1 + x_2 + \cdots + x_n| \leq |x_1| + |x_2| + \cdots + |x_n|$ $(x_1, x_2, \ldots, x_n \in \mathbb{R})$.
   (j) Si $n > 0$ entonces $\sqrt{n} \leq \sum_{i=1}^{n} 1/\sqrt{i}$.
   (k) Si $n > 0$ entonces $1 + 3 + \cdots + (2n - 1)$ es un cuadrado perfecto.
3. Demuestre por inducción que, para todo $n > 0$, dados los conjuntos $A_1, \ldots, A_n$, son verdaderas las siguientes igualdades:
   (a) $(A_1 \cap A_2 \cap \cdots \cap A_n)^c = A_1^c \cup A_2^c \cup \cdots \cup A_n^c$.
   (b) $(A_1 \cup A_2 \cup \cdots \cup A_n)^c = A_1^c \cap A_2^c \cap \cdots \cap A_n^c$.

4. Sea $n \in \mathbb{N}^*$ y sean $A_1, A_2, \ldots A_n$ conjuntos. Demuestre que es verdadero que $A_1 \triangle A_2 \triangle \cdots \triangle A_n = S_n$, en donde

   $$S_n = \{x : x \text{ pertenece a un número impar de } A_1, A_2, \ldots, A_n\}.$$

   En otras palabras, demuestre que para todo x es verdadero que $x \in A_1 \triangle A_2 \cdots \triangle A_n$ si y sólo si el conjunto $\{i : 1 \leq i \leq n, x \in A_i\}$ tiene un número impar de elementos.

5. Demuestre por inducción que, para todo $n \in \mathbb{N}^*$, se cumplen las siguientes afirmaciones:

   (a) $(1)(2) + (2)(3) + \cdots + (n)(n+1) = \frac{n(n+1)(n+2)}{3}$.
   (b) $(1)(1!) + (2)(2!) + \cdots + (n)(n!) = (n+1)! - 1$.
   (c) $\frac{1}{(1)(3)} + \frac{1}{(3)(5)} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$.
   (d) $\frac{1}{2^2-1} + \frac{1}{3^2-1} + \cdots + \frac{1}{(n+1)^2-1} = \frac{3}{4} - \frac{1}{2(n+1)} - \frac{1}{2(n+2)}$.

6. Dados $a, b \in \mathbb{Z}$, diremos que a es divisible por b (o a es múltiplo de b) si $b \neq 0$ y a es de la forma xb, con $x \in \mathbb{Z}$. Demuestre que para todo $n \in \mathbb{N}$ vale lo siguiente:

   (a) $n^3 - n$ es múltiplo de 6.
   (b) $a_n = 2^{2n+1} + 1$ es divisible por 3.
   (c) $a_n = 11^n - 4^n$ es divisible por 7.
   (d) $a_n = 9^n - 1$ es múltiplo de 8.
   (e) Si n es un impar positivo, entonces 2^n es divisible por 8.
   (f) Si $n > 0$ entonces $11^{n+1} + 12^{2n-1}$ es múltiplo de 133.
   (g) 7 divide a $8^n - 1$.
   (h) $5^{2n+1} + 1$ es divisible por 6.
   (i) $3^n + 7^n - 2$ es divisible por 8.
   (j) Si $n > 0$ entonces 4 es un divisor de $3^{2n-1} + 1$.

7. Demuestre por inducción que dados $a \in \mathbb{N}$ y $b \in \mathbb{N}^*$ existen $k, r \in \mathbb{N}$ tales que $a = bk + r$ y $r < b$. (*Ayuda*: haga inducción en a.)

8. Demuestre que dados $a, b, c \in \mathbb{N}$, si c es un divisor de a y c es un divisor de b, entonces c es un combinación lineal entera entre a y b, es decir, c es de la forma $xa + yb$ con $x, y \in \mathbb{N}$.

9. Demuestre por inducción que para todo $n \in \mathbb{N}$, n es divisible por 9 si y sólo si la suma de los dígitos de n es divisible por 9.

10. Demuestre por inducción que para todo $n \in \mathbb{N}$, n es divisible por 4 si y sólo si el número r_n es divisible por 4, donde r_n es el número formado por los últimos dos dígitos de n (por ejemplo, si $n = 1765$ entonces $r_n = 65$).

11. Sea p una propiedad, y suponga que

    (a) $p(3)$ es verdadera, y

    (b) para todo número natural n, si $p(n)$ es verdadera, entonces $p(n+1)$ también lo es.

    Demuestre que entonces $p(n)$ es verdadera para todo $n \geq 3$. (*Ayuda*: razone por contradicción y utilice el hecho de que $\mathbb{N}$ es un buen orden. También: sea $A = \{n \in \mathbb{N} : p(n+3) \text{ es verdadero } \}$. Demuestre que $A = \mathbb{N}$.)

12. Dado un número entero z, sea I_z el siguiente principio:

    Principio 2.16 (I_z). Sea $A \subseteq \mathbb{Z}^{\geq z}$ tal que $z \in A$ y para todo n, $n \in A$ implica $n+1 \in A$. Entonces $A = \mathbb{Z}^{\geq z}$.

    Demuestre que para todo z entero, I_z es equivalente a I_0 (note que I_0 es el PI).

13. Dado un orden lineal $(A, <)$ con un elemento mínimo (que llamaremos 0 por comodidad), formule el PIF para A, y demuestre (si es que es cierto) que este principio es equivalente a decir que $(A, <)$ es un buen orden.

14. Dado un conjunto A, sea $A^+ = A \cup \{A\}$. Diremos que un conjunto I es *inductivo* si para todo $X \in I$, $X^+ \in I$. Definimos el conjunto ω de esta manera:

    $$\omega := \{x : x \in I \text{ para todo conjunto inductivo } I \text{ tal que } \varnothing \in I\}.$$

    (a) Demuestre que $\varnothing \in \omega$.

    (b) Demuestre que ω es un conjunto inductivo.

    (c) Demuestre que ω cumple con el PI: para todo $A \subseteq \omega$, si $\varnothing \in A$ y A es inductivo, entonces $A = \omega$.

15. Hasta ahora habíamos manejado una noción intuitiva e informal sobre los números naturales. Ahora podemos *definir* al conjunto $\mathbb{N}$ de los números naturales así: $\mathbb{N} := \omega$ (véase la definición de ω en el ejercicio anterior). Además, definimos:

    (i) $0 := \varnothing$ (note que $\varnothing \in \omega$).

    (ii) Si $n \in \omega$, $n+1 := n^+ = n \cup \{n\} \in \omega$.

    Por ejemplo, $1 = 0+1 = 0^+ = 0 \cup \{0\} = \varnothing \cup \{\varnothing\} = \{\varnothing\}$; $2 = 1^+ = 1 \cup \{1\} = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}$. En general, n será un conjunto "con n elementos". Por la parte (c) ejercicio anterior, el PI es realmente un teorema y no un axioma.

    (a) Escriba explícitamente los primeros seis números naturales (estos son conjuntos).

(b) Demuestre por inducción que para todo número natural $n > 0$, $n = \{0, \ldots, n-1\}$ (de modo que todo número natural es subconjunto de $\mathbb{N}$).

(c) Demuestre que para todo $n \in \mathbb{N}, n \subseteq \mathcal{P}(\mathbb{N})$.

16. Definimos el orden $<$ en ω así: $n < m$ si y sólo si $n \in m$ (note que según esta definición $n < n+1$, pues $n \in n \cup \{n\} = n^+ = n+1$).

(a) Demuestre por inducción que el orden definido es irreflexivo y transitivo.

(b) Diremos que $n \leq m$ si y sólo si ($n < m$ o $n = m$). Demuestre que $\leq$ es antisimétrico (utilice inducción matemática).

(c) Demuestre que las relaciones $\leq$ y $\subseteq$ coinciden en $\mathbb{N}$, es decir, que dados números naturales n y m, $n \leq m$ si y sólo si $n \subseteq m$.

17. Ejercicios de combinaciones lineales:

(a) Una pulga puede avanzar mediante dos tipos de saltos: uno que la hace avanzar 2 cm, y otro que la hace avanzar 5 cm. Demuestre que para todo $n \in \mathbb{N}$, con $n > 3$, la pulga puede moverse exactamente n cm a partir de varios saltos.

(b) Una pulga puede avanzar mediante dos tipos de saltos: uno que la hace avanzar 5 cm, y otro que la hace avanzar 7 cm. Demuestre que para todo $n \in \mathbb{N}$, con $n > 23$, la pulga puede moverse exactamente n cm a partir de varios saltos.

(c) Una pulga puede avanzar mediante dos tipos de saltos: uno que la hace avanzar 15 cm, y otro que la hace avanzar 22 cm. Encuentre el mínimo $N \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ con $n > N$, la pulga puede moverse exactamente n cm a partir de varios saltos. Demuestre que en efecto se cumple esta última afirmación.

18. Demuestre que si en un país (visto como un conjunto finito de ciudades) se tiene que para todo par de ciudades distintas existe un único camino *de una sola vía* que las une, entonces es posible construir una ruta a partir de estos caminos que pase por cada ciudad exactamente una vez.

19. Demuestre que todo orden lineal finito es un buen orden. (*Ayuda*: haga inducción en $n =$ "N° de elementos del orden".)

§ 2.3 Definiciones por recursión

n!: *Factorial*

La operación *factorial*, es una función[2] que le asocia a cada número natural n un número natural, llamado *n factorial*, denotado como $n!$. La definición es la siguiente:

$$n! := n(n-1)(n-2)\cdots(3)(2)(1), \text{ para } n > 0.$$

Por convención, $0! = 1$. Por ejemplo, $1! = 1$ y $4! = (4)(3)(2)(1) = 24$.

Una manera más formal de definir a la función factorial es *recursivamente*, esto es, con una definición base y una definición inductiva:

(a) Definición base: si $n = 0$, entonces $n! = 1$.

(b) Definición inductiva: $(n+1)! = (n+1)(n!)$.

El lector puede percatarse del parecido entre una definición recursiva y el PI. Por ejemplo, para calcular 5! utilizamos esta definición y concluimos que:

$$5! = (4+1)! = (4+1)(4!) = (5)(4!).$$

Hemos *reducido* el problema de calcular 5! al de calcular 4!. Ahora,

$$4! = (3+1)! = (3+1)(3!) = (4)(3!);$$
$$3! = 3(2!);$$
$$2! = (2)(1!);$$
$$1! = (1)(0!).$$

Finalmente, gracias a que el conjunto de los números naturales es un buen orden, hemos llegado al 0 y por definición, $0! = 1$. Pero entonces:

$$1! = (1)(1) = 1;$$
$$2! = (2)(1!) = (2)(1) = 2;$$
$$3! = (3)(2!) = (3)(2) = 6;$$
$$4! = (4)(3!) = (4)(6) = 24; \text{ y así,}$$
$$5! = (5)(4!) = 5(24) = 120.$$

Para definir una función R por recursión debe especificarse su valor en 0 y después una descripción o fórmula de su valor en $n+1$, en la que se utiliza como recurso el valor de R en n. Veamos un ejemplo:

[2] El concepto de función será definido con detalle en el capítulo 4. Por ahora diremos que una función es un objeto que transforma elementos de un conjunto en elementos de otro conjunto. Por ejemplo, la función $\alpha(x) = 2x$ transforma números en el doble de ellos.

Ejemplo 2.17. Sea R la función definida recursivamente como $R(0) = -3$ y $R(n+1) = n + R(n)$. Calcule los primeros cuatro valores que toma R.

Solución.

$$\begin{aligned} &R(0) = -3; \quad \text{(por definición)} \\ &R(1) = R(0+1) = 0 + R(0) = 0 + (-3) = -3; \\ &R(2) = R(1+1) = 1 + R(1) = 1 + (-3) = -2; \\ &R(3) = R(2+1) = 2 + R(2) = 2 + (-2) = 0. \end{aligned}$$

Las operaciones básicas de suma y producto en los números naturales pueden ser definidas recursivamente (ejercicio 1). La exponenciación también. Por ejemplo, la función $R(n) = 2^n$ puede definirse recursivamente así:

$$\begin{aligned} R(0) &= 1; \\ R(n+1) &= 2R(n) \qquad (n \in \mathbb{N}). \end{aligned}$$

Por ejemplo, para calcular $2^3 = R(3)$, hacemos lo siguiente:

$$\begin{aligned} R(3) &= (2)(R(2)) \\ &= (2)(2)(R(1)) \\ &= (2)(2)(2)R(0) \\ &= (2)(2)(2)(1) = 8. \end{aligned}$$

Σ: Notación de sumatoria

Para el siguiente ejemplo es conveniente introducir una notación para sumar varios números entre sí, a saber, la *notación de sumatoria*. Si queremos sumar cinco números a_1, a_2, a_3, a_4 y a_5, simbolizamos el resultado de dicha operación así:

$$\sum_{i=1}^{5} a_i,$$

lo que se lee "sumatoria desde $i = 1$ hasta 5 de a_i".[3] De esta manera tenemos que

$$\sum_{i=1}^{5} a_i = a_1 + a_2 + a_3 + a_4 + a_5,$$

[3] Al igual que sucede con la notación para la unión e intersección generalizadas, es corriente hallar los términos de la sumatoria desplazados hacia la derecha, así: $\sum_{i=1}^{5} a_i$.

mientras que

$$\sum_{m=2}^{4} a_m = a_2 + a_3 + a_4.$$

También, por ejemplo,

$$\sum_{k=2}^{5} k^2 = 2^2 + 3^2 + 4^2 + 5^2 = 54,$$

y "la suma de los primeros siete números impares" es

$$\sum_{n=1}^{7} (2n-1), \quad \text{o también} \sum_{0\le j\le 6} 2j+1.$$

Supongamos que queremos expresar en notación de sumatoria la suma de los primeros cinco múltiplos de 3 positivos, esto es, $s = 3+6+9+12+15$. Para ello simplemente escribimos:

$$s = \sum_{i=1}^{5} 3i.$$

Note que también podemos escribir:

$$s = \sum_{n=1}^{5} 3n,$$

pues la escogencia de la variable en la expresión es irrelevante. A este tipo de variables se las conoce como *variables mudas*. Además, si es el caso que $A = \{1,2,3,4,5\}$ y $f(i) = 3i$, entonces podemos definir s también como

Variable muda

$$s = \sum_{i\in A} f(i), \quad \text{o también } s = \sum_{n\in A} f(n),$$

y esta expresión se lee "la suma de los $f(i)$, con $i \in A$".

☞ **Antes de seguir leyendo**

1. Escriba en notación de sumatoria "la suma de los primeros ocho números naturales pares".
2. Escriba en notación de sumatoria "la suma de los mayores seis números impares negativos".
3. Calcule $\sum_{i=2}^{6} i(-1)^{i+2}$.
4. Demuestre que $\sum_{i=1}^{5}(a_i + b_i) = \sum_{i=1}^{5} a_i + \sum_{i=1}^{5} b_i$.
5. Demuestre que $\sum_{i=1}^{5}(i+2) = \sum_{j=3}^{7} j$.
6. Sea $B = \{-5,-1,0,1,2,3,5,6\}$ y $f(x) = x^2$. Calcule $\sum_{a\in B} f(a)$.

Es natural que para demostrar ciertas propiedades de funciones definidas recursivamente sea necesario utilizar el PI. Veamos un ejemplo:

Ejemplo 2.18. Demuestre que para todo $n \geq 3$,

$$n! \geq 1 + \cdots + n = \sum_{i=1}^{n} i.$$

Solución. Debemos demostrar una propiedad para todos los números naturales *a partir de* 3. Es fácil ver que podemos modificar levemente el PI de modo que comencemos con el 3 como el caso base y mantengamos idéntico el paso inductivo, con la hipótesis adicional de que $n \geq 3$, para concluir que cierta propiedad es verdadera para todos los números naturales mayores o iguales que 3. (Véase el ejercicio 11 de la § 2.4.)

(a) Caso base ($n = 3$): $3! = 6 \geq 1 + 2 + 3 = \sum_{i=1}^{3} i$.

(b) Paso inductivo: supongamos que $n \geq 3$ es tal que $n! \geq \sum_{i=1}^{n} i$. Si sumamos $n + 1$ a ambos lados, obtenemos

$$n! + (n+1) \geq \sum_{i=1}^{n} i + (n+1) = 0 + 1 + \cdots + n + (n+1).$$

Por otro lado,

$$(n+1)! = (n+1)n! = n(n!) + n! \geq 2n + n! \geq (n+1) + n!.$$

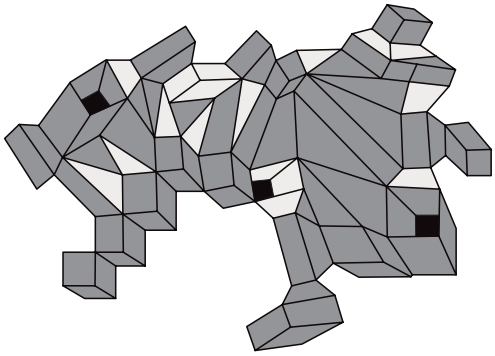
Aquí hemos utilizado el hecho de que $n \geq 3$ para afirmar que $n! \geq 2$. De las dos desigualdades anteriores concluimos que

$$(n+1)! \geq 1 + \cdots + n + (n+1) = \sum_{i=1}^{n+1} i,$$

como queríamos demostrar.

En virtud del PI, modificado levemente, concluimos que, para todo $n \geq 3$, $n! \geq \sum_{i=1}^{n} i$. ■

Ejercicios



1. Sea $S(n) = n + 1$, para $n \in \mathbb{N}$. S se llama la *función sucesor*.
   (a) Dado $m \in \mathbb{N}$, defina recursivamente la función "sumar m", esto es, $f_m(n) = m + n$. Para esto utilice la función sucesor.
   (b) Mediante la función f_m de la parte anterior, ¿cómo definiría recursivamente la función "producto por m": $p_m(n) = mn$?
2. Para todo $i \in \mathbb{N}$, sea a_i un número real.
   (a) Defina de manera recursiva la función g definida así:
   $$g(n) = \sum_{i=0}^{n} a_i = a_0 + a_1 + \cdots + a_n.$$
   (b) Exprese $s(m,n) = \sum_{i=m}^{n} a_i$ $(m \leq n)$, en términos de g.
3. La *sucesión*[4] *de Fibonacci*, $(f_n)_{n\in\mathbb{N}}$, se define recursivamente así:
   $$f_0 = f_1 = 1,$$
   $$f_n = f_{n-2} + f_{n-1} \quad (n \geq 2).$$
   Demuestre para todo $n \in \mathbb{N}$:
   (a) Si $n \geq 2$, entonces $f_0^2 + f_1^2 + f_2^2 + \cdots + f_n^2 = f_n \cdot f_{n+1}$.
   (b) Si $n \geq 1$, entonces f_{3n-1} es par.
   (c) Si $n \geq 1$, entonces f_{4n-1} es divisible por 3.
   (d) Si $n \geq 1$, entonces $f_{n-1} \cdot f_{n+1} = f_n^2 - (-1)^n$.
   (e) $f_n^2 + f_{n+1}^2 = f_{2n+2}$.
   (f) $f_{n+m+1} = (f_{m+1} \cdot f_n) + (f_{n+1} \cdot f_m) - (f_m \cdot f_n)$.

[4] Para el concepto de sucesión, véase la Definición 3.32, abajo.

4. Considere la función f que convierte números naturales en palabras formadas a partir de la letra A, definida recursivamente de esta manera:

$$\begin{aligned} &\text{(i)} && f(0) = A; \\ &\text{(ii)} && f(n+1) = Af(2n-1)A \quad (n > 0). \end{aligned}$$

Por ejemplo,

$$f(3) = Af(2)A = AAf(1)AA = AAAf(0)AAA = AAAAAAA.$$

Sea $g(n)$ =“número de letras A que aparecen en la palabra $f(n)$”. Encuentre una fórmula para $f(n)$ en términos de n y demuestre mediante inducción que su fórmula es válida. (*Ayuda*: la definición de $f(n)$ se hace por casos, según la paridad de n.)

5. Sea f una función que convierte números naturales en palabras formadas a partir de la letra B, definida recursivamente así:

$$\begin{aligned} &\text{(i)} && f(0) = B; \\ &\text{(ii)} && f(2n) = Bf(2n-1)B \quad (n > 0); \\ &\text{(iii)} && f(2n+1) = f(2n)Bf(2n) \quad (n > 0). \end{aligned}$$

Por ejemplo,

$$\begin{aligned} f(3) = f(2)Bf(2) = Bf(1)BBBf(1)B \\ = Bf(0)Bf(0)BBBf(0)Bf(0)B = BBBBBBBBBBB. \end{aligned}$$

Sea $g(n)$ =“número de letras B que aparecen en la palabra $f(n)$”. Encuentre una fórmula para $f(n)$ en términos de n y demuestre mediante inducción que su fórmula es válida. (*Ayuda*: la definición de $f(n)$ es por casos, según la paridad de n.)

6. Sea f una función que convierte números naturales en palabras formadas a partir de las letras A, B, definida recursivamente así:

$$\begin{aligned} &\text{(i)} && f(0) = BA; \\ &\text{(ii)} && f(1) = BAB; \\ &\text{(iii)} && f(n) = f(n-1)A \quad (n > 0 \text{ es par}); \\ &\text{(iv)} && f(n) = f(n-1)B \quad (n > 0 \text{ es impar}). \end{aligned}$$

Por ejemplo,

$$f(3) = f(2)B = f(1)AB = BABAB.$$

Demuestre mediante inducción que para todo $n \in \mathbb{N}$, n es par si y sólo si la palabra $f(n)$ tiene la misma cantidad de letras A que de letras B.

7. Dado $n \in \mathbb{N}^*$, sea τ_n el mínimo número de pasos para convertir la palabra $A_1A_2\cdots A_n$ en $A_nA_{n-1}\cdots A_1$, en donde cada paso consiste en permutar dos letras adyacentes. Por ejemplo, $\tau_2 = 2$ y $\tau_3 = 3$. Determine una fórmula para τ_n en términos de n y demuestre por inducción que es correcta.

8. Dado n natural positivo, sea v_n el mínimo número de pasos para convertir cualquier matriz cuadrada A de $n \times n$ en su transpuesta A^t, donde cada paso consiste en permutar dos casillas adyacentes ortogonalmente. Por ejemplo, $v_2 = 3$ y $v_3 = 13$. Determine una fórmula para v_n en términos de n y demuestre por inducción que esta fórmula es correcta. (Para más información sobre matrices, véase [8], o consulte el proyecto al final del capítulo 4, abajo.)
9. Dado $n \in \mathbb{N}$, K_n es el grafo formado por n puntos o vértices, y entre dos puntos distintos cualquiera una arista o línea. Sea e_n el número de aristas de K_n. Por ejemplo, $e_0 = e_1 = 0$, $e_2 = 1$, $e_3 = 3$ y $e_4 = 6$.

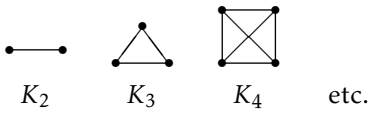


Figura 2.1 : K_n, el grafo completo de n vertices.

   (a) Encuentre una fórmula recursiva para e_n (comience en $n = 2$).
   (b) Demuestre por inducción que para todo n, $2e_n = n(n-1)$.

10. Consideremos la Figura 2.2, de las torres de Hanoi.[5]

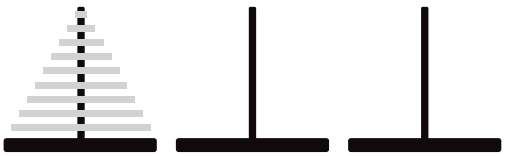


Figura 2.2 : Las torres de Hanoi (se ilustra el caso $n = 9$).

En ella se ilustran tres estacas; en la de la izquierda hay n discos de distintos tamaños, ordenados de menor a mayor diámetro. Queremos trasladar todos los discos a la estaca de la derecha, mediante movimientos de discos de una estaca a otra, obedeciendo las siguientes reglas:

   (i) Podemos mover un disco siempre y cuando éste no tenga otro(s) disco(s) sobre él.
   (ii) Podemos mover un disco hacia una nueva estaca siempre y cuando no haya discos más pequeños que él en esta estaca.

[5] Para más información, consulte `http://www.mazeworks.com/hanoi/`

(iii) Cuando movemos un disco de una estaca a otra, tal disco quedará encima de todos los discos (posiblemente ninguno) de la estaca.

Teniendo en cuenta esto, responda las siguientes preguntas:

(a) Si $n = 3$, calcule el mínimo número de movimientos de discos que se necesitan para trasladar los 3 discos a la estaca de la derecha.

(b) Para todo n, sea $f(n)$ el mínimo número de movimientos de discos que se necesitan para trasladar n discos a la estaca de la derecha. Encuentre una fórmula para $f(n)$ en términos de n y demuestre que para todo n esta fórmula es válida.

11. Un *triominó* es una región construida a partir de tres cuadrados de 1×1, unidos como muestra la Figura 2.3.

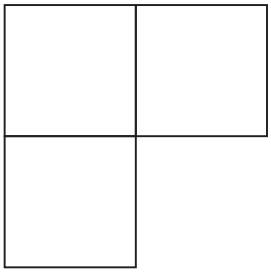


Figura 2.3 : Triominó.

Demuestre que cualquier tablero de $2^n \times 2^n$ ($n \in \mathbb{N}^*$) puede ser cubierto exactamente con un cuadrado de 1×1 junto con uno o más triominós.

§ 2.4 Isomorfismos entre estructuras ordenadas

La noción de similitud estructural o isomorfismo es central en matemáticas. En este caso dirigiremos nuestra atención hacia isomorfismos entre dos órdenes lineales. La siguiente definición es informal y será precisada más adelante:

Sean $(A_0, \leq_0)$ y $(A_1, \leq_1)$ órdenes lineales. Diremos que estos órdenes son *isomorfos*, lo que simbolizaremos $(A_0, \leq_0) \cong (A_1, \leq_1)$, si existe una forma de emparejar entre sí a *todos* los elementos de ambos órdenes, de modo que este emparejamiento preserve la estructura del orden.

Veamos un ejemplo en el cual se ilustra un isomorfismo entre órdenes:

Ejemplo 2.19. Sea $A_0 = 3\mathbb{N} = \{0, 3, 6, \dots\}$ con su orden usual y sea $A_1 = \{1, 3, 5, 7, \dots\}$, también con su orden usual. Veamos que estos órdenes son isomorfos: para ello construimos el siguiente emparejamiento entre los elementos de A_0 y A_1 (véase la figura de abajo).

Note que tal emparejamiento preserva el orden: por ejemplo, en el conjunto A_0 se tiene que $6 \leq 9$ y, al observar las parejas correspondientes en A_1 (5 y 7), se mantiene el orden: $5 \leq 7$. Otra forma de expresar que el orden se preserva consiste en observar que las líneas punteadas del dibujo anterior nunca se cruzan.

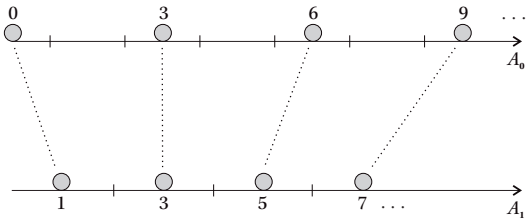


Figura 2.4: Emparejamiento entre A_0 y A_1.

Consideremos otro ejemplo:

Ejemplo 2.20. Sea z un número entero. Recordemos que:

$$\mathbb{Z}^{\geq z} := \{n \in \mathbb{Z} : n \geq z\}.$$

Demostremos que $(\mathbb{Z}^{\geq z}, \leq) \cong (\mathbb{N}, \leq)$. Definimos un emparejamiento entre los órdenes $\mathbb{Z}^{\geq z}$ y $\mathbb{N}$ por medio de la fórmula $\alpha(n) = n - z$ para $n \in \mathbb{Z}^{\geq z}$. Intuitivamente α es una traslación de $|z|$ unidades hacia la derecha o izquierda, dependiendo del signo de z. Verifiquemos que $\alpha : \mathbb{Z}^{\geq z} \to \mathbb{N}$ es un isomorfismo (véase la figura de la página siguiente). Para $a, b \in \mathbb{Z}^{\geq z}$, $a < b \leftrightarrow a - z < b - z$, pues sumar o restar un mismo número a ambos lados de una desigualdad la preserva, si y sólo si $\alpha(a) < \alpha(b)$.

El emparejamiento α hace evidente el hecho de que el conjunto $\mathbb{Z}^{\geq z}$ junto con su orden es en esencia la estructura ordenada de los números naturales, con la salvedad de que se utilizan nombres distintos para sus elementos. En la siguiente figura se muestra el caso en el cual $z = -2$.

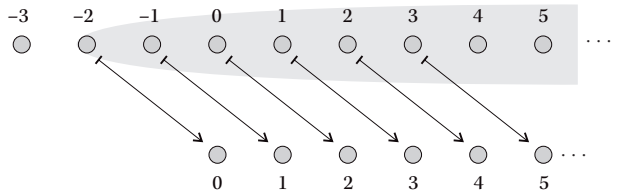


Figura 2.5: Se muestran dos estructuras ordenadas: $(\mathbb{Z}^{\geq 2}, \leq)$ y $(\mathbb{N}, \leq)$. Abajo, el 0 es el primer elemento. Arriba, el 0 es el tercer elemento. Sin embargo, esto no impide que en ambos casos se presente esencialmente la misma estructura.

Veamos ahora un ejemplo de dos órdenes que no son isomorfos:

Ejemplo 2.21. Sean $A_0 = \mathbb{Z}$ y $A_1 = \mathbb{N}$, ambos conjuntos con su orden usual. Podemos afirmar que A_0 y A_1 no son isomorfos (véase la figura de abajo). La razón es que ningún emparejamiento entre ambos conjuntos podrá preservar el orden: en cualquier dibujo que hagamos en el cual se intente emparejar ambos conjuntos resultarán líneas punteadas que se crucen; esto sucede fundamentalmente porque A_0 no tiene un elemento mínimo, mientras que A_1 sí lo tiene.

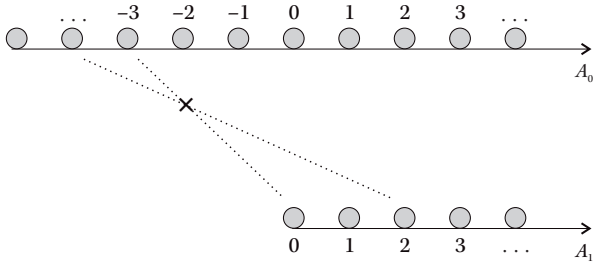


Figura 2.6: Es fácil convencerse de que cualquier intento de emparejamiento ordenado entre las estructuras A_0 y A_1 fracasará.

El enfoque que le hemos dado a esta sección ha sido intuitivo e informal, y nos hemos referido a dibujos para justificar el hecho de que dos estructuras son o no isomorfas. La definición formal del isomorfismo entre estructuras ordenadas es la siguiente:

Definición 2.22 (Isomorfismo entre estructuras ordenadas). Dadas dos estructuras ordenadas $(A_1, \leq_1)$, $(A_2, \leq_2)$, diremos que son *isomorfas*, y lo simbolizamos $(A_1, \leq_1) \cong (A_2, \leq_2)$, si existe una función α de A_1 en A_2 que cumple con las siguientes propiedades: *Isomorfismo*

(a) α es una *biyección*, esto es, para todo $b \in A_2$, existe un único $a \in A_1$ tal que $\alpha(a) = b$; y

(b) α es un *homomorfismo* entre órdenes, esto es, para todo par de elementos $a_1, a_2 \in A_1$, $a_1 \leq_1 a_2$ si y sólo si $\alpha(a_1) \leq_2 \alpha(a_2)$.

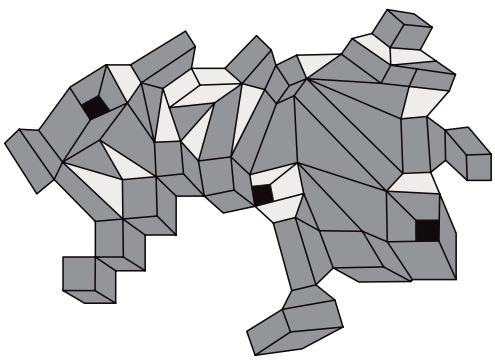
A la función α la llamamos un *isomorfismo entre órdenes*.

El siguiente teorema afirma que para todo n finito hay esencialmente un solo orden lineal con n elementos:

Teorema 2.23. Dos órdenes lineales finitos son isomorfos si y sólo si sus conjuntos base tienen el mismo número de elementos.

Prueba. Se deja al lector (ejercicio 8). ∎

Ejercicios



1. Demuestre que si $(A_1, <_1) \cong (A_2, <_2)$, entonces $(A_1, <_1)$ es un buen orden si y sólo si $(A_2, <_2)$ es un buen orden (en otras palabras, la propiedad *ser un buen orden* es una propiedad estructural.)
2. Para este ejercicio tenga en cuenta el concepto de conjunto inductivo (Definición 2.8).

(a) Dé un ejemplo de un conjunto inductivo A tal que $A \neq \varnothing$ y A sea un subconjunto *propio* de $\mathbb{N}$.

(b) Demuestre que si $A \subseteq \mathbb{N}$ es un conjunto inductivo y no vacío, entonces $(\mathbb{N}, <) \cong (A, <)$.

3. En este ejercicio se verá que es muy fácil clasificar a los subconjuntos inductivos en $\mathbb{N}$.

   (a) Demuestre que para todo A tal que $\varnothing \neq A \subseteq \mathbb{N}$, A es inductivo si y sólo si existe $n \in \mathbb{N}$ tal que $A = \{n, n+1, n+2, \dots\}$.

   (b) Sea $(\mathcal{G}_1, \preceq_1)$ la estructura ordenada dada por $\mathcal{G}_1 = \{A : A \text{ es un subconjunto inductivo de } \mathbb{N}\}$, con el orden $\preceq_1$ definido por $A \preceq_1 A'$, si y sólo si $A \subseteq A'$. Sea $(\mathcal{G}_2, \preceq)$ la estructura ordenada dada por $\mathcal{G}_2 = \{0, 1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}, \dots\}$, donde $\preceq_2$ el es $\leq$ usual en $\mathbb{R}$. Demuestre que $(\mathcal{G}_1, \preceq_1) \cong (\mathcal{G}_2, \preceq_2)$.

4. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:

   (a) Todo subconjunto infinito de $\mathbb{Z}$ es isomorfo a $\mathbb{N}$.

   (b) Todo subconjunto infinito de $\mathbb{N}$ es isomorfo a $\mathbb{N}$.

5. Demuestre que $\mathbb{R}$ y $(0, \infty)$ son órdenes isomorfos, ambos con el orden usual.

6. Sea $n = 2 \cdot 3 \cdot 5 = 30$. Dibuje un diagrama de los siguientes órdenes:

   (a) $(D_{30}^{+}, |)$; (b) $(\mathcal{P}(\{0,1,2\}), \subseteq)$.

   ¿Son ambos órdenes isomorfos?

7. Para cada par de estructuras ordenadas, determine si son isomorfas entre sí. En caso afirmativo, establezca un emparejamiento entre ellas. En caso negativo, provea una razón contundente por la cual no puede existir un isomorfismo entre ellas.

   (a) $(\{2,5,9\}, \leq) \overset{?}{\cong} (\{-1, \sqrt{2}, 100\}, \leq)$

   (b) $(\{1,2,3,6\}, \leq) \overset{?}{\cong} (\{-2,5,8,12,15\}, \leq)$

   (c) $(\{1,2,3\}, \leq) \overset{?}{\cong} (\mathbb{N}, \leq)$

   (d) $(\mathbb{N}, \leq) \overset{?}{\cong} (5\mathbb{N}, \leq)$

   (e) $(\mathbb{Z}, \leq) \overset{?}{\cong} (\mathbb{N}, \leq)$

   (f) $(\mathbb{Z}^{-}, \leq) \overset{?}{\cong} (\{a \in \mathbb{Z} : a \leq 9\}, \leq)$

   (g) $(\mathbb{Z}^{+}, \leq) \overset{?}{\cong} (\mathbb{Z}^{-}, \leq)$

   (h) $(\mathbb{R}^{+}, \leq) \overset{?}{\cong} (\mathbb{R}^{-}, \leq)$

(i) $(\mathbb{Z}, \leq) \overset{?}{\cong} (\mathbb{Q}, \leq)$

(j) $(\mathbb{Q}, \leq) \overset{?}{\cong} (\mathbb{R}, \leq)$

8. Demuestre el Teorema 2.23. (*Ayuda*: la prueba de *necesidad* (dirección $\leftarrow$) de este teorema se hace por inducción en n = "el número de elementos de los conjuntos base".)

§ 2.5 Conteo mediante inducción

El *conteo* en matemáticas intenta responder a preguntas como "cuántos objetos tienen cierta propiedad p" o, dicho de otro modo, "de cuántas formas distintas podemos construir un objeto con cierta propiedad especial". En esta sección ilustraremos cómo la inducción matemática puede servirnos como instrumento para contar.

Primero formalizamos, por inducción, la noción de que un conjunto tenga n elementos, en donde $n \in \mathbb{N}$:

Definición 2.24. Sea $n \in \mathbb{N}$ y A un conjunto. Definimos inductivamente la afirmación *A tiene n elementos*, así:

(a) ($n = 0$) Diremos que A tiene 0 elementos si y sólo si $A = \varnothing$.

(b) Diremos que A tiene $n+1$ elementos si y sólo si $A \neq \varnothing$ y para todo $a \in A$, $A \setminus \{a\}$ tiene n elementos.

Conjunto finito
Conjunto infinito

Definición 2.25. Diremos que un conjunto A es *finito* si existe $n \in \mathbb{N}$ tal que A tiene n elementos. Esto lo abreviamos así: $|A| = n$, lo que se lee: "el cardinal de A es igual a n". Si A no es finito, diremos que A es *infinito*.

Por ejemplo, $|\{1, 6\}| = 2$, $|\{1, 2, 2, 4\}| = 3$ y $|\varnothing| = 0$. Para demostrar que un conjunto es infinito, debemos demostrar que *no* tiene n elementos, para todo $n \in \mathbb{N}$. Veamos un ejemplo:

Teorema 2.26. Para todo $n \in \mathbb{N}$ vale lo siguiente: para todo $k \in \mathbb{N}$,

$$|\mathbb{N}^{\geq k}| \neq n,$$

en donde $\mathbb{N}^{\geq k} := \{x \in \mathbb{N} : x \geq k\}$).

Prueba. Demostramos el teorema mediante inducción en n:

(a) Caso base ($n = 0$): sea $k \in \mathbb{N}$: como $k \in \mathbb{N}^{\geq k}$, entonces este conjunto no es vacío, luego por definición $|\mathbb{N}^{\geq k}| \neq 0$.

(b) Paso inductivo: supongamos que la afirmación vale para n, esto es, que

$$\forall k \in \mathbb{N}, |\mathbb{N}^{\geq k}| \neq n.$$

Demostremos que la afirmación vale para $n+1$. Sea $k \in \mathbb{N}$ y supongamos, buscando una contradicción, que $|\mathbb{N}^{\geq k}| = n+1$. Esto implica, por la Definición 2.24, que $|\mathbb{N}^{\geq k} \setminus \{k\}| = n$. Sin embargo,

$$\mathbb{N}^{\geq k} \setminus \{k\} = \{k+1, k+2, \dots\} = \mathbb{N}^{\geq k+1}.$$

Pero la hipótesis de inducción implica que $|\mathbb{N}^{\geq k+1}| \neq n$, lo cual es una contradicción. Concluimos que $|\mathbb{N}^{\geq k}| \neq n+1$. ∎

Como corolario[6] de este teorema obtenemos el siguiente resultado:

Corolario 2.27. El conjunto $\mathbb{N}$ es infinito.

Prueba. Por el Teorema 2.26 se tiene que para todo n, $|\mathbb{N}^{\geq 0}| \neq n$. Esto implica por la Definición 2.25 que $\mathbb{N}^{\geq 0}$ es infinito. Pero claramente $\mathbb{N}^{\geq 0} = \mathbb{N}$. ∎

Veamos un ejemplo de un problema de conteo:

Ejemplo 2.28. Se dispone de 5 letras $\{a, b, c, d, e\}$ y se quiere escoger exactamente dos de ellas. ¿Cuántas elecciones distintas tenemos para hacer esto?

Solución. Lo primero que hacemos es plantear el problema en términos matemáticos. La pregunta formulada es esencialmente la siguiente: ¿cuántos subconjuntos del conjunto $B = \{a, b, c, d, e\}$ tienen exactamente 2 elementos? Por notación, a dichos conjuntos los llamaremos *2-conjuntos*. Sea $\mathcal{P}_2(B)$ el conjunto de todos los $X \subseteq B$, tales que B es un 2-conjunto, esto es,

$\mathcal{P}_2(B)$

$$\mathcal{P}_2(B) := \{X \in \mathcal{P}(B) : |B| = 2\}.$$

Listemos todos los elementos de $\mathcal{P}_2(B)$:

$$\{a,b\}, \{a,c\}, \{a,d\}, \{a,e\},$$
$$\{b,c\}, \{b,d\}, \{b,e\},$$
$$\{c,d\}, \{c,e\},$$
$$\{d,e\}.$$

[6] Un *corolario* es un teorema que es consecuencia directa de uno o varios teoremas anteriores. La distinción entre *lema*, *teorema* y *corolario* es relativa, pues en realidad todos ellos son proposiciones matemáticas verdaderas que tienen demostración.

Entonces hay exactamente $1+2+3+4=10$ 2-conjuntos que son subconjuntos de B. Como $\mathcal{P}(B)$ tiene $2^5=32$ subconjuntos, podemos entonces decir que si tomamos un subconjunto de B al azar, suponiendo que cada uno tiene la misma probabilidad de ser elegido; por lo tanto, la probabilidad de que éste sea un 2-conjunto es de $\frac{10}{32}$, aproximadamente 31 %. ■

Para contar el número de objetos que tienen cierta propiedad es conveniente imaginar que se está construyendo, por pasos o etapas, un objeto típico con tal propiedad. Precisamente es en este aspecto en donde las definiciones por recursión constituyen una poderoso instrumento para responder a preguntas sobre conteo.

Supongamos, por ejemplo, que estamos interesados en contar el número de subconjuntos de $A := \{a,b,c,d,e,f\}$ que son 2-conjuntos. Sea $B := \{a,b,c,d,e\}$, un conjunto más simple que A. Es claro que todo subconjunto de B es un subconjunto de A. Por lo tanto, podemos contar los subconjuntos de A que son 2-conjuntos de la siguiente forma:

$$\begin{aligned}(\text{N° de 2-conjuntos en } A) = (\text{N° de 2-conjuntos en } B)\\ + (\text{N° de 2-conjuntos en } A \text{ que } \textit{no} \text{ están en } B).\end{aligned}$$

Este enfoque es conveniente porque en el ejemplo 2.28 ya hemos calculado el número de 2-conjuntos contenidos en B. Resta calcular el número de 2-conjuntos contenidos en A que *no* están contenidos de B. Un objeto de este tipo necesariamente será de la forma $\{x,f\}$, con $x \in A$, y es fácil ver que existen exactamente 5 objetos con esta propiedad:

$$\{a,f\},\{b,f\},\{c,f\},\{d,f\},\{e,f\}.$$

Por ende,

$$|\mathcal{P}_2(A)| = |\mathcal{P}_2(B)| + 5 = 10 + 5 = 15.$$

Como el lector puede anticipar, a partir de un razonamiento análogo podremos concluir que si $C = \{a,b,c,d,e,f,g\}$, entonces:

$$|\mathcal{P}_2(C)| = |\mathcal{P}_2(A)| + 6 = 15 + 6 = 21.$$

Es razonable hacer entonces la siguiente conjetura general: si un conjunto A tiene n elementos (con $n > 1$), entonces A contiene un total de $1+2+\cdots+(n-1)$ subconjuntos que son 2-conjuntos. Demostremos esta afirmación mediante inducción matemática:

Teorema 2.29. Para todo $n \in \mathbb{N}$ con $n > 1$, si $|A| = n$, entonces

$$|\mathcal{P}_2(A)| = 1+\cdots+(n-1).$$

Prueba. Hacemos inducción en n:

(a) Caso base ($n = 2$): si $|A| = 2$, entonces el único subconjunto de A que es un 2-conjunto es A mismo. Luego la propiedad se verifica (pues $n - 1 = 1$).

(b) Paso inductivo: supongamos que la propiedad vale para n y demostrémosla para $n + 1$. Debemos demostrar que si $|A| = n + 1$, entonces A tiene $1 + \cdots + ((n + 1) - 1) = 1 + \cdots + n$ conjuntos que son 2-conjuntos. Sea A un conjunto tal que $|A| = n + 1$, digamos $A = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$. Sea $B = A \setminus \{a_{n+1}\}$. Queremos contar todos los subconjuntos de A que son 2-conjuntos. Estos se dividen en dos clases:

   (i) Los subconjuntos de B que son 2-conjuntos: por hipótesis de inducción ($|B| = n$), hay $1 + 2 + \cdots + (n - 1)$ de ellos.

   (ii) Los subconjuntos de A que son 2-conjuntos y *no* son subconjuntos de B: para que un conjunto X cumpla que $X \subseteq A$ y $X \nsubseteq B$ debe ocurrir que $a_{n+1} \in X$. Por ende, los conjuntos que consideramos aquí serán de la forma $X = \{x, a_{n+1}\}$, con $x \in B$. De estos habrá uno por cada elemento $x \in B$; como $|B| = n$, concluimos que hay n subconjuntos de A que son 2-conjuntos y no son subconjuntos de B.

Si sumamos, concluimos que A tiene un total de

$$(1 + \cdots + (n - 1)) + n = 1 + \cdots + n$$

subconjuntos que son 2-conjuntos, como se quería. ∎

Corolario 2.30. Para $n > 1$, si $|A| = n$, entonces $|\mathcal{P}_2(A)| = n(n - 1)/2$.

Prueba. Es una consecuencia del Teorema 2.29 y el ejemplo 2.11. ∎

El razonamiento inductivo es útil para formular una conjetura (véanse los comentarios previos al Teorema 2.29) y también para intentar demostrarla. Obviamente es común formular conjeturas razonables que resultan siendo falsas. Hasta los mejores matemáticos han creído que ciertas afirmaciones son verdaderas hasta que se descubre un contraejemplo para ellas. Las conjeturas que pueden demostrarse dejan de ser conjeturas y se convierten en teoremas, como es el caso del Teorema 2.29.

En este orden de ideas, podemos afirmar que el razonamiento inductivo es un método de *descubrimiento* o formulación de hipótesis, y también un método de *fundamentación* o demostración de teoremas.

Teorema 2.31. Para todo $n \in \mathbb{N}^*$, el número de formas distintas de ordenar linealmente un conjunto de n elementos es $n!$.

Prueba. Demostramos el resultado por inducción en n.

(a) Caso base ($n = 1$): sea A un conjunto con un solo elemento. Entonces claramente hay una única forma de ordenar linealmente a A. Luego el resultado es válido.

(b) Paso inductivo: supongamos que el resultado es verdadero para n y demostrémoslo para $n+1$. Sea A un conjunto de $n+1$ elementos,

$$A = \{a_1, a_2, \ldots, a_n, a_{n+1}\}.$$

Sea $B = A \setminus \{a_{n+1}\}$. Por hipótesis de inducción hay $n!$ formas distintas de ordenar linealmente a B. Consideremos cualquiera de estos órdenes: $a_{i_1} < a_{i_2} < \cdots < a_{i_n}$ con $a_{i_j} \in B$ para $j = 1, \ldots, n$. Podemos extender este orden a un orden lineal sobre A de $n+1$ formas distintas, según *ubiquemos* a a_{n+1} con respecto al orden previo:

$$\begin{aligned}
&\boldsymbol{a_{n+1}} < a_{i_1} < a_{i_2} < \cdots < a_{i_n},\\
&a_{i_1} < \boldsymbol{a_{n+1}} < a_{i_2} < \cdots < a_{i_n},\\
&\cdots,\\
&a_{i_1} < a_{i_2} < \cdots < \boldsymbol{a_{n+1}} < a_{i_n},\\
&a_{i_1} < a_{i_2} < \cdots < a_{i_n} < \boldsymbol{a_{n+1}}.
\end{aligned}$$

Además, es fácil ver que cualquier orden lineal sobre A se puede construir de la forma recién descrita, es decir, a partir de un orden lineal sobre B. Resumiendo, tenemos $n!$ distintos órdenes lineales sobre B y por cada uno de ellos, $n+1$ formas distintas de ubicar a a_{n+1}. Por consiguiente, el número de formas para ordenar linealmente a A será

$$\underbrace{(n+1) + (n+1) + \cdots + (n+1)}_{n! \text{ veces}} = (n+1)n! = (n+1)!,$$

como queríamos demostrar. ∎

Ejemplo 2.32. Calcule de cuántas formas distintas pueden hacer una fila cinco personas.

Solución. Sea $A = \{a_1, a_2, a_3, a_4, a_5\}$ el conjunto de las cinco personas. Una fila de estas cinco personas consiste esencialmente en ordenar linealmente a A. Por consiguiente habrá tantas filas, cuantos órdenes lineales sobre A, esto es, $5! = 120$. Podemos representar tantas filas

cuantas tuplas de A^5 en las cuales no se repiten sus entradas. Veamos algunos ejemplos:

$$(a_1, a_4, a_3, a_5, a_2),$$
$$(a_4, a_1, a_3, a_2, a_5),$$
$$(a_3, a_2, a_1, a_5, a_4),$$
$$(a_4, a_3, a_2, a_1, a_5),$$
$$(a_5, a_4, a_3, a_2, a_1),$$
$$\ldots$$

Teorema 2.33. Sea A un conjunto tal que $|A| = n$ y sea $k \in \mathbb{N}^*$. Entonces el conjunto de tuplas $A^k := \{(a_1, a_2, \ldots, a_k) : a_1, a_2, \ldots, a_k \in A\}$ tiene n^k elementos.

Prueba. Se deja al lector (ejercicio 3). ∎

Supongamos ahora que disponemos de los números $\{1, 2, \ldots, n\}$ y queremos extraer k de ellos (donde $1 \leq k \leq n$) para construir un orden lineal. ¿Cuántos órdenes lineales podemos hacer de esta forma? Un razonamiento informal es el siguiente:

1. Para elegir el primer elemento del orden tenemos n posibilidades distintas.
2. Para elegir el segundo elemento del orden tenemos $n-1$ posibilidades distintas, pues ya hemos elegido un elemento.
3. Para elegir el tercer elemento del orden tenemos $n-2$ posibilidades distintas, pues ya hemos elegido dos elementos.
   ...
k. Para elegir el k-ésimo elemento del orden tenemos $n-(k-1)$ posibilidades distintas, pues ya hemos elegido $k-1$ elementos.

Por lo tanto, el número de órdenes lineales de tamaño k construidos a partir de un conjunto de n elementos será el *producto* de las posibilidades anteriores, esto es,

$$n(n-1)(n-2)\cdots(n-k+1) = \tfrac{n!}{(n-k)!}.$$

Note que si A es un conjunto con n elementos y $1 \leq k \leq n$, entonces elegir un orden lineal de k elementos a partir de elementos de A es esencialmente elegir una k-tupla $(a_1, a_1, \ldots, a_k) \in A^k$ tal que todos los a_i sean distintos. Al conjunto de todas estas tuplas lo llamaremos $A!(k)$:

$A!(k)$

$$A!(k) := \{(a_1, \ldots, a_k) \in A^k : \ a_s \neq a_t \text{ para todo } s \neq t\}.$$

☞ **Antes de seguir leyendo**

Sean $A = \{1, 2, 3, \ldots, 10\}$ y $B = \{(a, b, c) : a, b, c \in A \text{ y } a < b < c\}$. Calcule el número de elementos del conjunto B.

Teorema 2.34. Sean $n, k \in \mathbb{N}$ con $0 < k \leq n$. Entonces el conjunto $A!(k)$ tiene $\frac{n!}{(n-k)!}$ elementos.

Prueba. Se deja al lector (ejercicio 4). ∎

No es difícil ver que el Teorema 2.31 es en realidad un corolario del Teorema 2.34, si se toma $k = n$.

A continuación resumimos algunos de los principales hechos fundamentales sobre el conteo:

Teorema 2.35 (Resumen del conteo). Sean $n, k \in \mathbb{N}^*$ y sea A un conjunto tal que $|A| = n$. Entonces:

(a) $|A^k| = n^k$;

(b) $(k \leq n)\ |A!(k)| = \dfrac{n!}{(n-k)!}$;

(c) el conjunto A puede ser ordenado linealmente de $n!$ formas distintas, o, en otras palabras, $|A!(n)| = n!$;

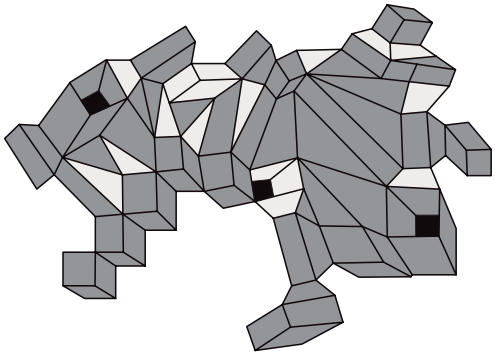
(d) $|\mathcal{P}(A)| = 2^n$;

(e) $|\mathcal{P}_2(A)| = \dfrac{n(n-1)}{2}$;

(f) $|\mathcal{P}_k(A)| = \dfrac{n!}{k!(n-k)!}$ (donde $\mathcal{P}_k(A) := \{X \in \mathcal{P}(A) : |X| = k\}$).

Prueba. Las partes (a), (b), (c) y (e) ya han sido discutidas en esta sección. La parte (d) se demostró en el ejercicio 8 de la § 1.2, mediante la representación de un subconjunto como una tupla de ceros y unos, pero también puede ser demostrada mediante inducción (ejercicio 7). Para la parte (f), véase el ejercicio 9, o una demostración mediante relaciones de equivalencia (Teorema 4.92.) ∎

Ejercicios



1. Demuestre que para todo $n \in \mathbb{N}$, si A y B son conjuntos tales que $A \subseteq B$ y A y B tienen n elementos, entonces $A = B$.
2. Para todo n, sea C_n el número de formas distintas de dividir a una región de dimensiones $2 \times n$ en distintas regiones rectangulares de dimensiones 2×1. En la figura se ilustra el caso para $n = 3$.

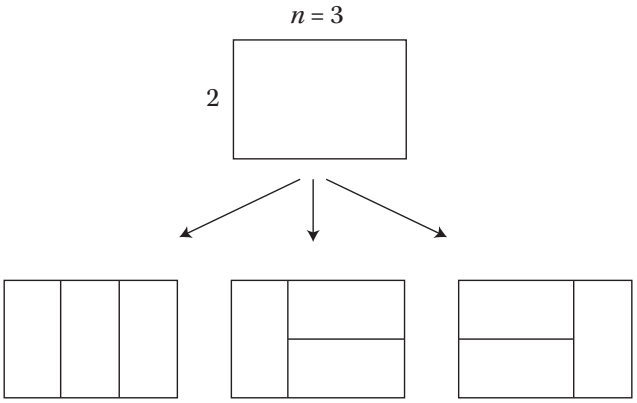


Figura 2.7: Caso $n = 3$: $C_n = 3$.

(a) Si $n > 2$, encuentre una fórmula recursiva para C_n en términos de algunos valores de C_k $(k < n)$.

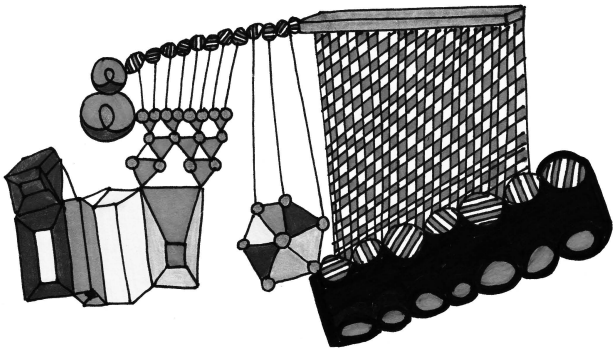
(b) Demuestre que la fórmula encontrada es válida.

(c) Demuestre que para todo $n \in \mathbb{N}^*$, C_{3n-1} es un número par.

(d) Demuestre que para todo $n \in \mathbb{N}^*$, C_{3n-1} es múltiplo de 3.

3. Demuestre el Teorema 2.33.
4. Demuestre el Teorema 2.34.
5. Sean $n, k \in \mathbb{N}$, con $k \leq n$, y sea A un conjunto tal que $|A| = n$. Demuestre que
$$|\mathcal{P}_k(A)| = |\mathcal{P}_{n-k}(A)|.$$
6. Demuestre que para todo $n \in \mathbb{N}$, n rectas que se encuentran en posición general (esto es, en donde ningún par de ellas son paralelas y no hay tres de ellas que pasen por el mismo punto) dividen al plano en un total de k regiones, donde k está dado por
$$k = 1 + \frac{n(n+1)}{2}.$$
7. Demuestre por inducción matemática que para todo $n \in \mathbb{N}$, si A es un conjunto tal que $|A| = n$, entonces $|\mathcal{P}(A)| = 2^n$.
8. Sea $n \in \mathbb{N}$, $n > 0$. Supongamos que disponemos de 5 colores distintos para colorear una bandera de n casillas, de modo que las casillas adyacentes sean coloreadas de distintos colores. En términos de n, ¿cuántas banderas distintas podemos construir? Demuestre el resultado que propuso mediante inducción matemática. (Aquí el orden sí importa: para $n = 3$, por ejemplo, la bandera dada por [Verde | Blanco | Naranja] es distinta de la bandera dada por [Naranja | Blanco | Verde].)
9. Demuestre que dados $n, k \in \mathbb{N}$, si $k \leq n$ entonces
$$|\mathcal{P}_k(A)| = \frac{n!}{k!(n-k)!}.$$
(*Ayuda*: haga inducción sobre n y, al considerar el paso inductivo de n a $n+1$, haga inducción sobre k, $k = 0, 1, \ldots, n+1$. Al considerar el paso inductivo de k a $k+1$, examine dos casos: (i) $k+1 = n+1$: este caso es sencillo. (ii) $k+1 \leq n$: observe que si $A' \subseteq A$, A' tiene n elementos, A tiene $n+1$ elementos y $A \setminus A' = \{a\}$, entonces $\mathcal{P}_{k+1}(A)$ es la unión entre $\mathcal{P}_{k+1}(A')$ y $\{a \cup S : S \in \mathcal{P}_k(A')\}$. A partir de lo anterior, deduzca que
$$|\mathcal{P}_{k+1}(A)| = |\mathcal{P}_{k+1}(A')| + |\mathcal{P}_k(A')|,$$
y utilice la hipótesis de inducción para $n, k+1$ y para n, k.)

Proyecto: Axiomas de Peano



En este proyecto estudiaremos las propiedades algebraicas de los números naturales a partir de los llamados *Axiomas de Peano*. [7] Estos axiomas capturan las propiedades esenciales de la estructura de los números naturales, de las cuales se deducen muchas otras. En este sentido este proyecto consiste en deducir, a partir de ciertas propiedades básicas, llamadas *axiomas*, otras propiedades.

Definición 2.36. Diremos que una *estructura de Peano* es una estructura

$$(A, S, +, \cdot, <, 0_A),$$

en donde A es un conjunto, S es la operación unaria en A llamada la *función sucesor*, $+$ y $\cdot$ son operaciones binarias sobre A llamadas *suma* y *producto*, respectivamente, 0_A es un elemento de A (que por comodidad lo llamaremos simplemente 0) y, además, se cumplen los siguientes diez axiomas o propiedades:

- (A_1) Para todo $n \in A$, $S(n) \neq 0$.
- (A_2) Para todo $n, m \in A$, si $S(n) = S(m)$, entonces $n = m$.
- (A_3) Para todo $n \in A$, $n + 0 = n$.
- (A_4) Para todo $n, m \in A$, $n + S(m) = S(n + m)$.
- (A_5) Para todo $n \in A$, $n \cdot 0 = 0$.
- (A_6) Para todo $n, m \in A$, $n \cdot 0 = 0$.
- (A_7) Para todo $n, m \in A$, $n \cdot S(m) = (n \cdot m) + x$.
- (A_8) Para todo $n, m \in A$, $n < m$ si y sólo si existe $k \in A$ tal que $k \neq 0$ y $n + k = m$. Además, por convención diremos que $n \leq m$ si y sólo si $n < m$ o $n = m$.

[7] En realidad postularemos una versión ligeramente distinta de los Axiomas de Peano; en particular, incluimos la definición de la suma, el producto y el orden.

(A_9) Dada cualquier propiedad $p(n)$, si $p(0)$ es verdadera y para todo $n \in A$ vale que $p(n) \to p(S(n))$, entonces para todo $n \in A$, $p(n)$ es verdadera.

Puede verse que la estructura ω de los números naturales, definida explícitamente en el ejercicio 15 de la § 2.2, es una estructura de Peano, esto es, verifica los diez axiomas anteriores. Como se verá en los ejercicios, en *toda* estructura de Peano la suma es conmutativa. Como la estructura de los números naturales es una estructura de Peano, entonces concluimos que la suma de los naturales es conmutativa. Dicho de otro modo, la conmutatividad de la suma en la estructura de los números naturales no es válida simplemente por definición, sino que es un teorema.

Dado que las estructuras de Peano cumplen con el axioma de inducción (A_9), muchas de las propiedades que se pedirá demostrar en los ejercicios se harán mediante este axioma. Veamos, por ejemplo, que en una estructura de Peano se cumple que para todo $n \in A$, $0 + n = 0$. Para ello hacemos inducción en n:

(a) Caso base ($n = 0$): entonces $0 + n = 0 + 0 = n + 0 = 0$, en virtud del axioma A_3.

(b) Paso inductivo: sea $n \in A$ y supongamos que $0 + n = n$. Queremos ver que $0 + S(n) = S(n)$. Por A_4, $0 + S(n) = S(0 + n)$ y, por hipótesis de inducción, $S(0 + n) = S(n)$. Concluimos que $0 + S(n) = S(n)$.

Por el axioma de inducción (A_9) concluimos que, para todo $n \in A$, tenemos que $0 + n = n$.

Problemas

1. Demuestre las siguientes propiedades:
   (a) Para todo $n \in A$, $S(n) \neq n$.
   (b) Para todo $n \in A$, si $n \neq 0$ entonces existe m tal que $S(m) = n$.
   (c) Para todo $n \in A$, $0 \leq n$.
   (d) Para todo $n \in A$, si $n \neq 0$ entonces $0 < n$.
   (e) *Ausencia de elemento máximo:* para todo $n \in A$ existe $m \in A$ tal que $n < m$.
2. Demuestre las siguientes propiedades de la suma:
   (a) Para todo $n \in A$, $0+n = n$. (Intente hacer este ejercicio de nuevo, sin ver la solución arriba.)

(b) Para todo $n, m \in A$, $S(n) + m = S(n + m)$.

(c) *Conmutatividad:* para todo $n, m \in A$, $n + m = m + n$.

(d) *Asociatividad:* para todo $n, m, k \in A$, $n + (m + k) = (n + m) + k$.

3. Demuestre las siguientes propiedades del producto:

(a) Para todo $n \in A$, $0 \cdot n = 0$.

(b) Para todo $n, m \in A$, $S(n) \cdot m = (n \cdot m) + m$.

(c) *Conmutatividad:* para todo $n, m \in A$, $n \cdot m = m \cdot n$.

4. Definimos 1 como $1 := S(0)$. Demuestre las siguientes propiedades algebraicas:

(a) $0 \neq 1$.

(b) *Distributividad:* para todo $n, m, k \in A$, $n \cdot (m + k) = (n \cdot m) + (n \cdot k)$.

(c) *Distributividad:* para todo $n, m, k \in A$, $(n + m) \cdot k = (n \cdot k) + (m \cdot k)$.

(d) *Asociatividad:* para todo $n, m, k \in A$, $n \cdot (m \cdot k) = (n \cdot m) \cdot k$.

(e) Para todo $n, m, k \in A$, si $n + k = m + k$ entonces $n = m$.

(f) Para todo $n \in A$, $n + 1 = S(n)$.

(g) *Identidad:* Para todo $n \in A$, $n \cdot 1 = n$.

(h) Para todo $n, m, \in A$, si $n + m = 0$ entonces $n = m = 0$.

(i) Para todo $n, m, \in A$, si $n \cdot m = 0$ y $n \neq 0$ entonces $m = 0$.

(j) Para todo $n, m \in A$ Si $n + m = 1$ entonces $\{n, m\} = \{0, 1\}$.

(k) Para todo $n, m, \in A$, si $n \cdot m = 1$ entonces $n = 1$ y $m = 1$.

(l) *Ley Cancelativa:* para todo $n, m, k \in A$, si $k \neq 0$ y $k \cdot n = k \cdot m$ entonces $n = m$.

5. Demuestre las siguientes propiedades del orden:

(a) *Irreflexividad de $<$:* para todo $n \in A$ es falso que $n < n$.

(b) *Transitividad de $<$:* para todo $n, m, k \in A$, si $n < m$ y $m < k$ entonces $n < k$.

(c) *Reflexividad de $\leq$:* para todo $n \in A$ se tiene que $n \leq n$.

(d) *Antisimetría de $\leq$:* para todo $n, m \in A$, si $n \leq m$ y $m \leq n$ entonces $n = m$.

(e) *Transitividad de $\leq$:* para todo $n, m, k \in A$, si $n \leq m$ y $m \leq k$, entonces $n \leq k$.

6. Demuestre las siguientes propiedades:

(a) Para todo $n, m \in A$, $n < m$ si y sólo si $S(n) \leq m$.

(b) Para todo $n, m \in A$, $n \leq m$ si y sólo si $n < S(m)$.

(c) *Tricotomía:* para todo $n, m \in A$, $n < m$ o $m < n$ o $n = m$.

(d) Para todo $n, m \in A$, $n \leq m$ o $m \leq n$.

(e) Para todo $n, m \in A$, si $m \neq 0$ entonces $m \leq n \cdot m$.

(f) Para todo $n, m \in A$, si $m \neq 0$ entonces $n < n + m$.

(g) Para todo $n \in A$, $n < S(n)$.

(h) Para todo $n, m \in A$, $n < m$ si y sólo si $S(n) < S(m)$.

(i) Para todo $n, m \in A$, $n \leq m$ si y sólo si $S(n) \leq S(m)$.

(j) *Antidensidad de <:* para todo $n, m \in A$, no es verdadero que $n < m < S(n)$.

7. *Transporte de estructura*: sea X un conjunto de la forma

$$X = \{x_n : n \in \mathbb{N}\},$$

en donde para todo $n, m \in \mathbb{N}$, $n \neq m$ si y sólo si $x_n \neq x_m$.[8] En otras palabras: para todo x, $x \in X$ si y sólo si existe un único $n \in \mathbb{N}$ tal que $x = x_n$. Definimos la siguiente estructura sobre X:

(a) $0_X := x_0$;

(b) dado $x_n \in X$, $S_X(x_n) := x_{n+1}$;

(c) dados $x_n, x_m \in X$, $x_n +_X x_m := x_{n+m}$;

(d) dados $x_n, x_m \in X$, $x_n \cdot_X x_m := x_{nm}$;

(e) dados $x_n, x_m \in X$, $x_n <_X x_m$ si y sólo si $n < m$.

Demuestre que la estructura $(X, 0_X, S_X, +_X, \cdot_X, <_X)$ es una estructura de Peano, esto es, que verifica los nueve axiomas de la definición de estructuras de Peano.

8. Sean $(A, 0_A, S_A, +_A, \cdot_A, <_A)$ y $(B, 0_B, S_B, +_B, \cdot_B, <_B)$ estructuras de Peano. Demuestre que A y B son estructuras de Peano isomorfas. Esto es, demuestre que existe una función

$$f : A \to B$$

tal que f es un *isomorfismo entre estructuras de Peano*. En otras palabras, demuestre lo siguiente:

(a) f es una biyección, esto es, para todo $b \in B$ existe un único $a \in A$ tal que $f(a) = b$.

(b) f preserva la estructura de Peano. Más precisamente, dados $n, m \in A$ se tiene que:

(i) $f(0_A) = 0_B$;

[8] Un conjunto que pueda verse de la forma recién descrita es llamado un conjunto *enumerable*. En el capítulo 5 se estudiará en detalle ese tipo de conjuntos.

(ii) $f(S(n))S(f(n))$;

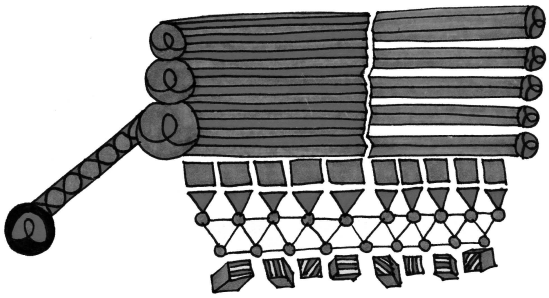
(iii) $f(n +_A m) = f(n) +_B f_m$;

(iv) $f(n \cdot_A m) = f(n) \cdot_B f_m$;

(v) $n <_A m$ si y sólo si $f(n) <_B f(m)$.

(c) Si $g : A \to B$ es un isomorfismo entre estructuras de Peano, entonces $f = g$.

Lecturas adicionales

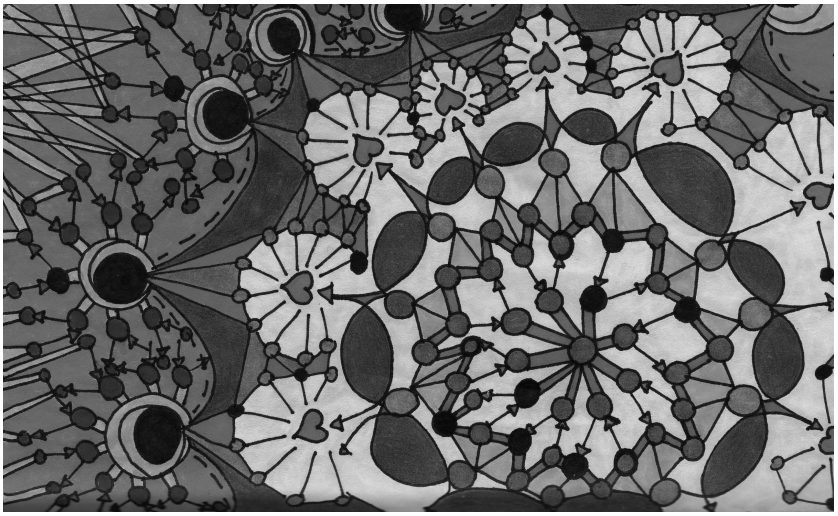


Se recomienda consultar las siguientes lecturas, con miras a profundizar en algunos de los temas tratados en este capítulo:

- Para más información sobre el PBO y la inducción matemática, consulte [8], §§ 2.4 y 2.5; [5], § 1.6; [6], § 2.7; [11], § 19.
- Para una exposición más general sobre buen orden e inducción, consulte [2], §§ 2.1 y 2.2.
- Para una introducción formal al conjunto de los números naturales, consulte [4], § 3.2.
- Para una exposición axiomática de los números naturales, basada en los axiomas de Peano, consulte [5], §§ 1.1–1.4; [7], cap. 3.
- Para más información sobre conteo y definiciones por recursión, consulte [6], cap. 3.

CAPÍTULO 3

DIVISIBILIDAD: LOS NÚMEROS ENTEROS



Estructuras algebraicas...

El orden usual sobre el conjunto de los números enteros se encuentra íntimamente relacionado con la operación de la suma: $a \leq b$ si y sólo si existe un número entero $e \geq 0$ tal que $a + e = b$. Dicho informalmente, a es menor o igual a b cuando puede *evolucionar* al sumarse con e y convertirse en b, el cual es un objeto más complejo. Por ejemplo, $2 \leq 7$ ya que existe $e \geq 0$ tal que $2 + e = 7$. Aquí se toma $e = 5$.

En este capítulo estudiaremos la teoría de una relación en los enteros, llamada la relación *divide*. Esta relación es evolutiva en el mismo orden de ideas del párrafo anterior, pero con respecto a la operación de multiplicación. Por ejemplo, el 2 puede evolucionar con la suma para convertirse en 7, y por eso $2 \leq 7$. Sin embargo, el 2 no puede hacer lo mismo con el producto, pues ningún número entero e verifica que $2e = 7$. Por ende, diremos que 2 *no divide* al 7 o que 2 *no es un divisor* de 7. Por otra parte, por ejemplo, el 3 puede evolucionar y convertirse en 12 al

multiplicarse por $e = 4$. En este orden de ideas, diremos que 3 es un divisor de 12.

La relación de divisibilidad permite definir el concepto de *residuo* módulo n. A partir de tal concepto estudiaremos más adelante, además, la llamada relación de *congruencia módulo n* entre números enteros y, con base en ella, definiremos una estructura numérica llamada $\mathbb{Z}_n$, *la estructura de los enteros módulo n*.

§ 3.1 Conceptos fundamentales y el Algoritmo de la División

Definición 3.1 (Relación *divide*). Dados $a, b \in \mathbb{Z}$, decimos que *a divide* a b,[1] y escribimos $a \mid b$, si y sólo si $a \neq 0$ y existe $e \in \mathbb{Z}$ tal que $ae = b$. Si a no divide a b, escribiremos $a \nmid b$.

|: *Divide*

Divisor *Múltiplo*

Dados $a, b \in \mathbb{Z}$, decimos que a es un *divisor* de b, o equivalentemente que b es un *múltiplo* de a, si $a \mid b$. Por ejemplo, 3 es un divisor de 30 (tomamos $e = 10$), 4 es un divisor de -8 (tomamos $e = -2$), -12 es múltiplo de -4 (tomamos $e = 3$) y por definición, para cualquier número entero a tenemos que a no es múltiplo de 0.

La primera observación importante que podemos hacer es que toda la información de la relación *divide* "se encuentra completamente" en el conjunto de los números enteros no negativos, es decir, en $\mathbb{N}$. Por ejemplo, la respuesta a la pregunta: ¿divide -4 a -326?, será la misma que la respuesta a la pregunta: ¿divide 4 a 326 ? En general, tenemos:

Lema 3.2. Sean $a, b \in \mathbb{Z}$. Las siguientes afirmaciones son equivalentes:

(a) $a \mid b$;
(b) $-a \mid b$;
(c) $-a \mid -b$;
(d) $a \mid -b$;
(e) $|a| \mid |b|$.[2]

Prueba. Se deja al lector (ejercicio 6). ∎

[1] No confundir con la expresión "a dividido por b" $= a/b$.

[2] La expresión $|a|$ denota el *valor absoluto* de a y se define de la siguiente manera: $|a| = a$ si $a \geq 0$, y $|a| = -a$ si $a < 0$.

Las siguientes son algunas de las propiedades básicas de la relación de divisibilidad:

Teorema 3.3. Dados $a, b, c \in \mathbb{Z}$ tenemos que

(a) $1 \mid a$;

(b) si $a \neq 0$, entonces $a \mid a$;

(c) si $b \neq 0$ y $a \mid b$, entonces $|a| \leq |b|$;

(d) si $a \mid b$ y $b \mid a$, entonces $|a| = |b|$;

(e) si $a \mid b$ y $b \mid c$, entonces $a \mid c$;

(f) si $c \mid a$ y $c \mid b$, entonces c divide a cualquier *combinación lineal* entera de a y b. (Una *combinación lineal* de a y b es un número de la forma $xa + yb$, con $x, y \in \mathbb{Z}$.)

Combinación lineal

Prueba.

(a) Dado que $1a = a$, entonces existe $e \in \mathbb{Z}$, $e = a$, tal que $1e = a$.

(b) Tomamos $e = 1$ y tenemos $ae = a1 = a$. Como $a \neq 0$, entonces por definición concluimos que $a \mid a$.

(c) Sea $e \in \mathbb{Z}$ tal que $ae = b$. Entonces $|a||e| = |b|$. Como $b \neq 0$, entonces $e \neq 0$, luego $1 \leq |e|$. Si multiplicamos a ambos lados por $|a|$, que es un número entero no negativo, obtenemos que $|a| \leq |a||e| = |b|$.

(d) De las hipótesis deducimos que $a, b \neq 0$. Esto junto con (c) implica que $|a| \leq |b|$ y $|b| \leq |a|$. Luego, por la antisimetría de $\leq$, concluimos que $|a| = |b|$.

(e) Sean e, f números enteros tales que $ae = b$ y $bf = c$. Entonces se tiene que $c = bf = (ae)f = a(ef)$. Luego, por definición, $a \mid c$; notemos que $a \neq 0$ pues $a \mid b$.

(f) Sean k, l números enteros tales que $ck = a$ y $cl = b$. Entonces se tiene que $xa + yb = x(ck) + y(cl) = ce$, en donde $e = xk + yl \in \mathbb{Z}$. Luego $c \mid (xa + yb)$. ∎

Corolario 3.4. Sean $n, a_1, a_2, \ldots, a_k, x_1, x_2, \ldots, x_k \in \mathbb{Z}$. Supongamos que para todo i con $1 \leq i \leq k$ tenemos que n divide a a_i. Entonces n divide la combinación lineal

$$\sum_{i=1}^{k} x_i a_i = x_1 a_1 + x_2 a_2 + \cdots + x_k a_k.$$

Prueba. Se deja al lector (ejercicio 7). ∎

La relación *divide* no es un orden parcial en $\mathbb{Z}$. En efecto, no es reflexiva, pues $0 \nmid 0$, ni es antisimétrica; por ejemplo, $2 \mid -2$ y $-2 \mid 2$,

pero $2 \neq -2$. Sin embargo, en el conjunto $\mathbb{N}^* = \mathbb{N} \setminus \{0\} = \{1, 2, 3, \dots\}$, la relación *divide* es un orden parcial.

Corolario 3.5. La estructura ordenada $(\mathbb{N}^*, |)$ es un orden parcial.

Prueba. La reflexividad, antisimetría y transitividad valen respectivamente por las partes (b), (d) y (e) del Teorema 3.3. ∎

El Algoritmo de la División

Cuando un número entero d, distinto de 0, no divide a otro número entero a, podemos en todo caso encontrar una aproximación a la división. Por ejemplo, si queremos repartir $a = 30$ alfajores de forma equitativa entre $d = 7$ duendes, podemos darle $e = 4$ dulces a cada duende y quedarnos con $r = 2$ alfajores, esto es, el *residuo*. En otras palabras, encontramos dos números e y r tales que $a = de + r$. En este caso, $30 = 7(4) + 2$. El siguiente teorema, fundamental en la teoría de números, afirma que siempre podemos hacer lo anterior, siendo a, d números enteros, no necesariamente números naturales, con $d \neq 0$, de forma que r sea un número natural *estrictamente* menor que $|d|$. En el caso de los alfajores y los duendes, esta última condición se traduce en justicia para con los duendes, ya que si el residuo fuera mayor o igual al número de duendes, entonces podríamos entregarle uno o más alfajores a cada uno de ellos.

Algoritmo de la División

Teorema 3.6 (Algoritmo de la División). Dados $a, d \in \mathbb{Z}$ con $d \neq 0$, existen dos números enteros únicos e y r tales que

$$a = de + r, \text{ con } 0 \leq r < |d|.$$

$\text{RES}_d(a)$: Residuo

El número r es llamado *el residuo que resulta al dividir a por d*, o *residuo de a módulo d*, y se denota así: $\text{RES}_d(a)$.

Prueba. Sea R el siguiente conjunto:

$$R = \{a - de : e \in \mathbb{Z}, a - de \geq 0\}.$$

Claramente $R \subseteq \mathbb{N}$ y, además, es un conjunto no vacío por lo siguiente:

(i) Si $a \geq 0$, tómese $e = 0$ y así $a - de = a \geq 0$.

(ii) Si $a < 0$, como $d \neq 0$, entonces tómese $e = a$ si $d > 0$, y $e = -a$ si $d < 0$. Entonces $a - de = a \pm da = a(1 \pm d)$, que por construcción será un número entero no negativo.

Por el PBO, R debe tener un elemento mínimo, que llamaremos r. Entonces existe $e \in \mathbb{Z}$ tal que $r = a - de$ y, por ende, $a = de + r$. Es claro,

además, que $r \geq 0$. Veamos ahora que $r < |d|$. Para esto procedamos por contradicción: supongamos que $r \geq |d|$, es decir, $r - |d| \geq 0$. Observemos además que

$$r - |d| = a - de - |d| = a - d(e \pm 1).$$

Esto significa que $r - |d| \in R$. Pero, como $d \neq 0$, $r - |d| < r$, esto contradice la minimalidad de r. Así pues, $r < |d|$. Hemos demostrado la existencia de e y r con las propiedades deseadas. Para demostrar que ellos son únicos con respecto a tales propiedades, supongamos que existen $e', r' \in \mathbb{Z}$ tales que $a = de' + r'$ con $0 \leq r' < |d|$. Entonces $de + r = a = de' + r'$. Hay dos casos, según cuál sea mayor entre r y r':

(i) $r \leq r'$: como $de + r = de' + r'$, entonces $d(e - e') = r' - r \leq r' < |d|$. La penúltima desigualdad es verdadera, dado que $r \geq 0$. Puesto que $d(e - e') = r' - r \geq 0$, concluimos que

$$|d| \cdot |e - e'| = d(e - e') < |d|,$$

luego $|e - e'| < 1$. Pero el único número natural menor que 1 es 0, así que $|e - e'| = 0$ y esto implica que $e = e'$. Además, tenemos que $r = a - de = a - de' = r'$.

(ii) $r' \leq r$: razonamos de forma análoga a como hicimos en (i) para concluir que $e = e'$ y $r = r'$.

En cualquier caso tenemos que $e = e'$ y $r = r'$. ∎

Ejemplo 3.7. Los siguientes son algunos ejemplos del Algoritmo de la División, esto es, de expresiones de la forma $a = de + r$, con $d \neq 0$ y $0 \leq r < |d|$:

(a) $0 = (4 \cdot 0) + 0$;
(b) $14 = (-3 \cdot -4) + 2$;
(c) $-14 = (-3 \cdot 5) + 1$;
(d) $-20 = (9 \cdot -3) + 7$;
(e) $20 = (9 \cdot 2) + 2$;
(f) $79 = (8 \cdot 9) + 7$;
(g) $15 = (3 \cdot 5) + 0$;
(h) $1 = (3 \cdot 0) + 1$.

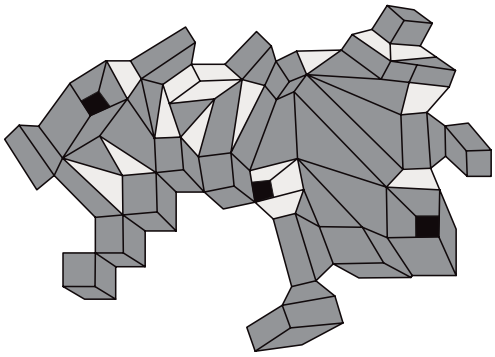
☞ **Antes de seguir leyendo**

Para cada uno de los números enteros a y d, encuentre $r = RES_d(a)$:

1. $a = 70$, $d = 12$;
2. $a = -40$, $d = 6$.
3. $a = 30$, $d = -8$.

Observación 3.8. En el Algoritmo de la División ($a = de + r$, $0 \leq r < |d|$) tenemos que el residuo $r = \text{RES}_d(a)$ es igual a 0 si y sólo si $d \mid a$.

Ejercicios



1. Recuerde que un número par es un número entero n tal que $2 \mid n$, es decir, un número de la forma $n = 2k$ (en donde $k \in \mathbb{Z}$). Un *impar* es un número entero que no es par. Decimos que los números pares tienen paridad 0 y los números impares tienen paridad 1. Si a y b son pares, y w y z son impares, determine la paridad de:
   (a) $a + b$,
   (b) $a + w$,
   (c) $w + z$,
   (d) ab,
   (e) wz,
   (f) az,
   (g) a^w $(a, w \in \mathbb{N}^*)$,
   (h) $w^a + w^z$ $(a, z \in \mathbb{N}^*)$,
   (i) $ab + wz$.
2. Demuestre que para todo número entero z, z y z^2 tienen la misma paridad. Generalice el resultado anterior para z y z^n y demuéstrelo por inducción matemática.
3. Demuestre que todo número $a \in \mathbb{Z}^*$ tiene un número infinito de múltiplos enteros y un número finito de divisores enteros.
4. Calcule todos los divisores de 240.
5. Dibuje el orden $(D_{210}^+, |)$.
6. Demuestre el Lema 3.2.
7. Demuestre el Corolario 3.4.
8. Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^*$. Demuestre que si $\text{RES}_n(a) = r$ y $\text{RES}_n(b) = s$, entonces $\text{RES}_n(ab) = \text{RES}_n(rs)$.

9. Encuentre $k, r \in \mathbb{Z}$ tales que $-178 = 13k + r$, $0 \leq r < 13$. A partir de esto encuentre $\text{RES}_{26}(-356)$.
10. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:
    (a) Si $a \mid b$ y $a' \mid b'$, entonces $aa' \mid bb'$.
    (b) Si $ka \mid kb$ entonces $a \mid b$.
    (c) Si $de \mid c$, entonces $d \mid c$.
    (d) Si $c \mid de$, entonces $c \mid d$.
11. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso ($a, b \in \mathbb{Z}, n \in \mathbb{N}^*$):
    (a) $\text{RES}_n(n^2) = 0$,
    (b) $\text{RES}_n(-a) = \text{RES}_n(a)$,
    (c) $\text{RES}_n(n-1) = n-1$,
    (d) $\text{RES}_n(a+b) = \text{RES}_n(a) + \text{RES}_n(b)$,
    (e) $\text{RES}_n(a+b) = \text{RES}_n(\text{RES}_n(a) + \text{RES}_n(b))$.
12. Si $d \neq 0$ y $a = de + r$, con $0 \leq r < |d|$, demuestre que uno solo de estos números enteros es múltiplo de d: $a, a+1, \ldots, a+|d|-1$.

§ 3.2 El máximo común divisor

Para esta sección necesitaremos establecer el siguiente resultado:

Lema 3.9. Todo conjunto finito A no vacío de números enteros tiene un elemento máximo que es único y que llamaremos $\text{MÁX}(A)$.

$\text{MÁX}(A)$: *Máximo de A*

Prueba. La prueba se puede hacer por inducción en el número de elementos del conjunto y se deja al lector (ejercicio 1). ∎

Dado $a \in \mathbb{Z}$, sea D_a el conjunto de todos los divisores de a:

D_a: *Divisores de a*

$$D_a := \{d \in \mathbb{Z} : d \mid a\}.$$

Por el Lema 3.2 y el Teorema 3.3, para todo $a \in \mathbb{Z}$ tenemos que $1 \in D_a$ y que $D_a = D_{-a}$. Además, $D_0 = \mathbb{Z}^*$, ya que para todo número entero $x \neq 0$, $x \mid 0$. Recordemos que dado $a \neq 0$, si $d \mid a$ entonces $|d| \leq |a|$ y por ende, $D_a \subseteq \{-|a|, \ldots, -1, 1, \ldots, |a|\}$. Luego D_a es un conjunto finito no vacío. Esto da pie a la siguiente definición:

(a,b): MCD *entre a y b*

Definición 3.10 (Máximo común divisor). Dados a, b números enteros, no ambos 0, definimos el *máximo común divisor*, o MCD, *entre a y b*, y lo denotamos (a,b), así:

$$(a,b) := \text{MÁX}(D_a \cap D_b).$$

La anterior definición tiene sentido, ya que el conjunto $D_a \cap D_b$ es finito y no vacío, así que por el Lema 3.9 tiene un único elemento máximo. Note que si $a = b = 0$, entonces $D_a \cap D_b = D_0 = \mathbb{Z}^*$ y este conjunto carece de un elemento máximo; por esto en la definición anterior exigimos que a y b no sean ambos 0. Para $a \neq 0$ tenemos que $(a,0) = \text{MÁX}(D_a \cap D_0) = \text{MÁX}(D_a) = |a|$. La última igualdad vale gracias al Teorema 3.3 (c).

En ocasiones nos referimos a (a,b) como $\text{MCD}(a,b)$. El lector notará que en general la expresión (a,b) puede significar cualquiera de los siguientes tres objetos:

(i) el intervalo abierto $(a,b) = \{x \in \mathbb{R} : a < x < b\}$;

(ii) el par ordenado (a,b) que lista a los elementos a y b;

(iii) el máximo común divisor entre a y b.

En general, el contexto determinará a cuál de los anteriores objetos nos refiramos al escribir (a,b). Por ejemplo, en esta sección lo más común será utilizar la expresión (a,b) para referirnos al máximo común divisor entre a y b.

> ☞ **Antes de seguir leyendo**
>
> Sean $a, b, d \in \mathbb{Z}$. Demuestre:
>
> 1. $(a,b) = (-a,b) = (-a,-b) = (a,-b) = (b,a)$.
> 2. Si $d \mid a$, entonces $(a,d) = |d|$.

Teorema 3.11 (El MCD como combinación lineal). Sean a y b dos enteros no ambos 0. Si $(a,b) = d$, entonces d es la mínima combinación lineal entera positiva entre a y b.

Prueba. Sea $C = \{ax + by : ax + by > 0,\ x, y \in \mathbb{Z}\}$ el conjunto de todas las combinaciones lineales enteras positivas entre a y b. Como a y b no son ambos nulos, entonces $aa + bb > 0$ y por ende, C es un subconjunto no vacío de $\mathbb{N}$. Sea m el elemento mínimo de C. Entonces existen $x, y \in \mathbb{Z}$ tales que $m = ax + by$. Veamos que $m = d$:

(a) $m \mid a$: por el Algoritmo de la División, sabemos que existen números enteros e y r tales que

$$a = me + r \qquad (0 \leq r < m).$$

Tenemos que

$$r = a - me = a - (ax + by)e = a(1 - ex) + b(-ye).$$

Entonces r es una combinación lineal entre a y b. Dado que $r < m$, por minimalidad de m concluimos que $r \notin C$ y esto implica que $r = 0$. Por ende, $a = me$ y $m \mid a$.

(b) $m \mid b$: la demostración es análoga a la realizada en (a).

(c) $m = d$: como $m \mid a$ y $m \mid b$, entonces $m \leq d$. Como $d \mid a$ y $d \mid b$, por el Teorema 3.3, $d \mid (ax + by)$, luego $d \leq ax + by = m$. Concluimos que $d = m$. ∎

☞ **Antes de seguir leyendo**

Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:

1. 12 es una combinación lineal entre 18 y 42.
2. Dados $a, b \in \mathbb{Z}$ no ambos 0 y $d = (a, b)$, existen los números enteros únicos x, y tales que $d = ax + by$.
3. Dados $a, b \in \mathbb{Z}$ tales que $a, b \neq 0$ y $d = (a, b)$, existen los números enteros x, y, x', y' tales que $d = ax + by = ax' + by'$ y, además, $x \neq x'$ o $y = y'$.

Teorema 3.12. Dados $a, b \in \mathbb{Z}$ no ambos 0, $D_a \cap D_b = D_{(a,b)}$.

Prueba. Utilizamos el método de doble inclusión:

(⊆) Si $x \in D_a \cap D_b$, entonces $x \mid a$ y $x \mid b$. Por el Teorema 3.3, x divide a cualquier combinación lineal de a y b, en particular, $x \mid (a, b)$.

(⊇) Si $x \in D_{(a,b)}$, entonces $x \mid (a, b)$. Como $(a, b) \mid a$ y $(a, b) \mid b$, obtenemos por transitividad que $x \mid a$ y $x \mid b$, luego $x \in D_a \cap D_b$. ∎

Este teorema tiene como consecuencia la siguiente caracterización del máximo común divisor entre a y b:

Teorema 3.13 (Caracterización del MCD). Dados a, b números enteros, $d = (a, b)$ si y sólo si valen las siguientes condiciones:

(a) $d > 0$;

(b) $d \mid a$, $d \mid b$ y para todo $e \in \mathbb{Z}$, si $e \mid a$ y $e \mid b$, entonces $e \mid d$.

Prueba. Utilizamos el método de doble implicación:

(→) Si $d = (a,b)$, entonces $d > 0$, $d \mid a$ y $d \mid b$ y si $e \mid a$ y $e \mid b$ entonces $e \in D_a \cap D_b = D_d$, es decir, $e \mid d$.

(←) Sabemos que $d \mid a$ y $d \mid b$, luego $d \in D_a \cap D_b$. Sea $e \in D_a \cap D_b$. Por tanto, $e \mid a$ y $e \mid b$, entonces por hipótesis $e \mid d$. Luego $e \leq |e| \leq |d| = d$. La última igualdad vale gracias a que $d > 0$. Entonces tenemos que $d = \text{MÁX}(D_a \cap D_b) = (a,b)$. ∎

Teorema 3.14. Si $d \neq 0$ y $a = de + r$, entonces $(a,d) = (d,r)$.

Prueba. Sea $m_a = (a,d)$ y $m_r = (d,r)$. Como $m_a \mid a$ y $m_a \mid d$, entonces $m_a \mid (a - de)$. Luego $m \mid r$ y así m_a es un divisor común de a y r. Por tanto $m_a \leq m_r$. De forma similar, $m_r \mid d$ y $m_r \mid r$, luego m_r divide a $de + r = a$. Así que m_r es divisor común de a y d; por lo tanto, $m_r \leq m_a$. Concluimos que $m_a = m_r$. ∎

El teorema anterior, junto con el Algoritmo de la División, sugieren una forma efectiva de calcular (a,d) cuando d no es 0. Sabemos que $a = de_1 + r_1$, con $0 \leq r_1 < |d|$. Si $r_1 = 0$, entonces $d \mid a$ y $(a,d) = |d|$. Si $r_1 > 0$, entonces utilizamos de nuevo el Algoritmo de la División, dividiendo d por r_1:

$$d = r_1 e_2 + r_2 \qquad (0 \leq r_2 < r_1).$$

Note que $|d| > r_1 > r_2 \geq 0$; así que si repetimos el proceso anterior varias veces, obtendremos residuos cada vez menores pero siempre mayores o iguales a 0. Por el PBO existe un número entero k tal que $r_k = 0$. En términos más formales:

$$\begin{aligned}
a &= de_1 + r_1 && (0 \leq r_1 < |d|),\\
d &= r_1 e_2 + r_2 && (0 \leq r_2 < r_1),\\
r_1 &= r_2 e_3 + r_3 && (0 \leq r_3 < r_2),\\
r_2 &= r_3 e_4 + r_4 && (0 \leq r_4 < r_3),\\
&\cdots,\\
r_{k-3} &= r_{k-2} e_{k-1} + r_{k-1} && (0 \leq r_{k-1} < r_{k-2}),\\
r_{k-2} &= r_{k-1} e_k + r_k && (0 \leq r_k < r_{k-1}).
\end{aligned}$$

Como $r_k = 0$, es el caso que $r_{k-1} \mid r_{k-2}$, es decir, $(r_{k-2}, r_{k-1}) = r_{k-1}$. Pero, por el Teorema anterior aplicado repetidamente, tenemos que

$$(r_{k-2}, r_{k-1}) = (r_{k-3}, r_{k-2}) = \cdots = (r_2, r_1) = (d, r_1) = (a,d),$$

de modo que $(a,d) = r_{k-1}$, el "penúltimo residuo del proceso".

Algoritmo de Euclides

Este resultado es conocido con el nombre de *Algoritmo de Euclides*. Éste es un método efectivo para calcular el MCD entre dos números enteros. Veamos algunos ejemplos:

Ejemplo 3.15. Calcule $(84, 30)$.

Solución. Si utilizamos el Algoritmo de Euclides, obtenemos:

$$\begin{aligned} 84 &= (30)2 + 24, \\ 30 &= (24)1 + 6, \\ 24 &= (6)4 + 0. \end{aligned}$$

Entonces $(84, 30) = 6$. A partir de las ecuaciones anteriores, concluimos que

$$6 = 30 - 24 = 30 - (-2(30) + 84) = (3)30 + (-1)84,$$

y hemos escrito a 6 como la mínima combinación lineal entera positiva entre 84 y 30.

Ejemplo 3.16. Calcule $(-35, -48)$.

Solución. Si utilizamos el Algoritmo de Euclides, obtenemos:

$$\begin{aligned} -35 &= (-48)1 + 13, \\ -48 &= (13)(-4) + 4, \\ 13 &= (4)3 + 1, \\ 4 &= (1)4 + 0. \end{aligned}$$

Entonces $(-35, -48) = 1$. Además, a partir de las ecuaciones anteriores obtenemos

$$\begin{aligned} 1 &= 13 - 3(4) = 13 - 3(-48 + 4(13)) = -3(-48) - 11(13) \\ &= -3(-48) - 11(-35 - 1(-48)) = 8(-48) + (-11)(-35), \end{aligned}$$

y hemos escrito a 1 como la mínima combinación lineal positiva entre -35 y -48.

Primos relativos

Definición 3.17 (Primos relativos). Dos números enteros a y b, no ambos 0, son *primos relativos* si $(a, b) = 1$.

Pensemos en dos números que no sean primos relativos, por ejemplo, 2 y 6. El lector podrá convencerse de que nunca podrá expresar al 1 como combinación lineal del 2 y el 6. La razón es que $(2, 6) = 2$, luego

cualquier combinación lineal entre 2 y 6 será un múltiplo de 2. Algo análogo ocurre, por ejemplo, con el 5 y el 10. En contraste, si tomamos dos primos relativos como 2 y 9, entonces podremos escribir a 1 como una combinación lineal de ellos:[3] $1 = (5)2 + (-1)9$. Recíprocamente, si podemos expresar a 1 como una combinación lineal de a y b, entonces necesariamente a y b son primos relativos.

Teorema 3.18. $(a,b) = 1$ si y sólo si existen $s,t \in \mathbb{Z}$ tales que $sa + tb = 1$.

Prueba. Utilizamos el método de doble implicación:

($\rightarrow$) Esta dirección la garantiza el Teorema 3.11.

($\leftarrow$) Como $(a,b) \mid a$ y $(a,b) \mid b$, por el Teorema 3.3 $(a,b) \mid sa + tb = 1$, luego $0 < (a,b) \leq 1$ y esto implica que $(a,b) = 1$. ∎

En general, si un número entero divide a un producto, no necesariamente divide a cada uno de los elementos que conforman este producto. Por ejemplo, $10 \mid (4)(15)$ pero $10 \nmid 4$ y $10 \nmid 15$. Sin embargo, si un número entero divide al producto entre dos números enteros y es primo relativo de alguno de ellos, entonces necesariamente divide al otro número entero:

Teorema 3.19. Dados $a,b,c \in \mathbb{Z}$, si $(a,b) = 1$ y $a \mid bc$, entonces $a \mid c$.

Prueba. Como $(a,b) = 1$, existen $s,t \in \mathbb{Z}$ tales que $1 = sa + tb$. Si multiplicamos la igualdad anterior por c, obtenemos que $c = sac + tbc$. Como $a \mid a$ y $a \mid bc$, entonces $a \mid c$, por el Teorema 3.3 (e). ∎

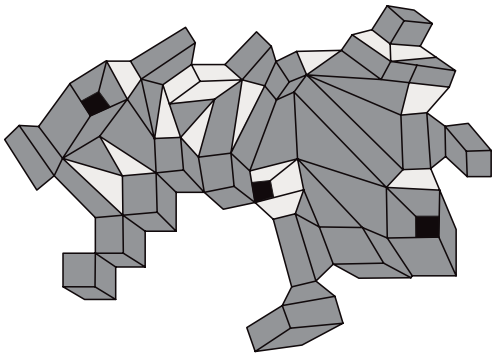
☞ **Antes de seguir leyendo**

Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:

1. Si a y b son primos relativos y b y c son primos relativos, entonces a y c son primos relativos.
2. Si $a \mid bc$ y $a \nmid b$, entonces $a \mid c$.
3. Si $(a,b) = 1$, $(a,c) = 1$ y $a \mid bcd$, entonces $a \mid d$.
4. Si $d = (a,b)$ y $a = dx$, entonces $(x,b) = 1$.
5. Si $d = (a,b)$, $a = dx$ y $b = dy$, entonces $(k,y) = 1$.

[3] Note que esta combinación lineal no tiene por qué ser única; por ejemplo, también se tiene que $1 = (-40)2 + (9)9$.

Ejercicios



1. Demuestre el Lema 3.9.
2. Para cada uno de los siguientes pares de números enteros a y b, halle $d = (-120, 176)$, y exprese este número como una combinación lineal entre a y b.
   (a) $a = 18$, $b = 12$;
   (b) $a = -120$, $b = 176$;
   (c) $a = 15$, $b = 72$;
   (d) $a = 3600$, $b = 1256$;
   (e) $a = 43$, $b = 44$;
   (f) $a = 120$, $b = 455$;
   (g) $a = 48$, $b = 50$;
   (h) $a = 3260$, $b = 888$.
3. Demuestre que dados $a, b, c \in \mathbb{Z}$, $(a, b) \mid c$ si y sólo si existen $x, y \in \mathbb{Z}$ tales que $ax + by = c$.
4. Demuestre las siguientes propiedades del MCD (donde $a, b, m \in \mathbb{Z}$, a y b no son ambos nulos y $m \neq 0$):
   (a) *Conmutatividad*: $(a, b) = (b, a)$.
   (b) *Distributividad*: $(ma, mb) = |m|(a, b)$.
   (c) *Asociatividad*: $((a, b), c) = (a, (b, c))$.
   (d) *Absorción*: $(a, (a, b)) = (a, b)$.
5. Demuestre las siguientes afirmaciones, en donde todos los números considerados son enteros:
   (a) $(a, b) = (a, b + ka)$.
   (b) Si $ab \mid cd$, y a y d son primos relativos, entonces $a \mid c$.
   (c) Si a y b son primos relativos, entonces $(a + b, a - b) \leq 2$.
   (d) Si $(a, x) = d$ y $(b, x) = 1$, entonces $(ab, x) = d$.
   (e) Si $a \mid c$ y $b \mid c$, entonces $\frac{ab}{(a,b)} \mid c$. (Aquí $\frac{ab}{(a,b)}$ se define como el número entero k tal que $k(a, b) = ab$.)

(f) Si $(a,x) = (b,x) = 1$, entonces $(ab,x) = 1$.

(g) Si $(a,x) = 1$ y $a \mid xy$, entonces $a \mid y$.

6. ¿Existen soluciones *enteras* a la ecuación $5^{200}x + 7^{500}y = 1$? ¿Y a la ecuación $12x + 35y = 137$? Justifique sus respuestas.

7. Demuestre las siguientes afirmaciones:

   (a) Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^*$, $(a,b) = 1$ si y sólo si $(a^n, b^n) = 1$.

   (b) Si $(a,b) = c$ y $(b,c) = 1$, entonces $(ac,b) = 1$.

   (c) Si $(a,x) = (b,x) = 1$, entonces $(ab,x) = 1$.

   (d) Cualesquiera dos números enteros consecutivos son primos relativos.

   (e) Para todo $n \in \mathbb{N}^*$, 2^n y 3^n son primos relativos. Además, para todo n encuentre explícitamente enteros a_n y b_n tales que $2^n a_n + 3^n b_n = 1$. (*Ayuda*: utilice inducción y recursión.)

8. Sea f la *sucesión de Fibonacci*, definida en el ejercicio 3 de la § 2.3 (p. 83, arriba). Pruebe por inducción en n que $(f_{n+1}, f_n) = 1$.

9. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:

   (a) Dados $a, b \in \mathbb{N}^*$, $((a,b),(c,d)) = ((a,c),(b,d))$.

   (b) Dados $a, b \in \mathbb{N}^*$, $a + b$ es primo si y sólo si $(a,b) = 1$. (En caso de que la afirmación sea falsa, determine si alguna de las dos implicaciones vale en general y en caso tal, demuéstrela.)

   (c) Si $(a,b) \neq 1$ y $(b,c) \neq 1$, entonces $(a,c) \neq 1$.

10. Demuestre que para todo $r \in \mathbb{Q}$, $r = \frac{a}{b}$ (con $a, b \in \mathbb{Z}$, $b \neq 0$) existen los números enteros únicos p y q tales que $(p,q) = 1$, $q > 0$ y $r = \frac{p}{q}$.

    (*Ayuda*: para la existencia, defina $q := \frac{|b|}{(a,b)}$; demuestre que $q \in \mathbb{Z}$. Defina p de manera análoga. Demuestre que $\frac{a}{b} = \frac{p}{q}$.)

11. Para este ejercicio considere la siguiente definición:

    Definición (clausura). Dado $A \subseteq \mathbb{Z}$, definimos el conjunto $\mathrm{CL}(A)$ (la *clausura* de A) así: $c \in \mathrm{CL}(A)$ si y sólo si existen $x_1, \ldots, x_n \in \mathbb{Z}$ y $a_1, \ldots, a_n \in A$ tales que $c = x_1 a_1 + \cdots + x_n a_n$.[4]

    Demuestre que para todo $A \subseteq \mathbb{Z}$ y $a, b \in \mathbb{Z}$ se cumplen las siguientes afirmaciones:

    (a) $0 \in \mathrm{CL}(A)$.

[4] Si $A = \varnothing$, definimos $\mathrm{CL}(A) = \{0\}$.

(b) Si $A \subseteq B$, entonces $\text{CL}(A) \subseteq \text{CL}(B)$.

(c) $A \subseteq \text{CL}(A)$.

(d) $\text{CL}(\text{CL}(A)) = \text{CL}(A)$.

(e) Existe $a \in \mathbb{Z}$ tal que $\text{CL}(A) = \text{CL}(\{a\})$. (*Ayuda*: si $\text{CL}(A) = \{0\}$, el resultado se tiene. De lo contrario, defina a como el mínimo elemento del conjunto $\mathbb{N}^* \cap \text{CL}(A)$, el cual existe por el PBO Como $a \in \text{CL}(A)$, verifique que por las partes (b) y (d) se tiene que $\text{CL}(\{a\}) \subseteq \text{CL}(A)$. Para la otra inclusión, comience por demostrar que todo número entero positivo que pertenezca a $\text{CL}(A)$ debe pertenecer a $\text{CL}(\{a\})$, por la minimalidad de a.)

(f) $\text{CL}(\{a, b\}) = \mathbb{Z}$ si y sólo si $(a, b) = 1$.

12. Para este ejercicio considere la siguiente definición:

Definición (MCD generalizado). Sea $A \subseteq \mathbb{Z}$ tal que $A \setminus \{0\} \neq \varnothing$. Definimos el MCD *del conjunto* A, y lo denotamos como $\text{MCD}(A)$, como el mayor número entero que divide a todos los elementos de A. Es decir,

$$\text{MCD}(A) := \text{MÁX}\Big(\bigcap_{a \in A} D_a\Big).$$

Note que, en particular, $(a, b) = \text{MCD}(\{a, b\})$; luego en realidad la definición de $\text{MCD}(A)$ es una generalización de la definición de (a, b) (Definición 3.10).

Demuestre las siguientes afirmaciones:

(a) Si $A \subseteq B \subseteq \mathbb{Z}$, entonces $\text{MCD}(B) \subseteq \text{MCD}(A)$.

(b) $\text{MCD}(\{x\}) = |x|$ (donde $x \in \mathbb{Z}^*$).

(c) $\text{MCD}(A)$ es el único número entero d que cumple con lo siguiente:

  (i) Para todo $a \in A$, $d \mid a$.

  (ii) Para todo x, si para todo $a \in A$ se tiene que $x \mid a$, entonces se tiene que $x \mid d$.

(d) $\text{MCD}(A) = \text{MÍN}(\text{CL}(A) \cap \mathbb{N}^*)$. En otras palabras, $\text{MCD}(A)$ es la mínima combinación lineal positiva de elementos de A. (Véase el ejercicio 11 para la definición de $\text{CL}(A)$.)

(e) $\text{MCD}(A) = \text{MCD}(\text{CL}(A))$.

(f) $\text{MCD}(A) = 1$ si y sólo si $\text{CL}(A) = \mathbb{Z}$.

(g) Si $a \in \mathbb{Z}^*$ y $A = \{ka : k \in \mathbb{Z}\}$, entonces $\text{MCD}(A) = |a|$.

(h) $\text{MCD}(A \cup \{x\}) = \text{MCD}(A)$ si y sólo si $x \in \text{CL}(A)$.

(i) $\text{MCD}(A \cup B) = (\text{MCD}(A), \text{MCD}(B))$.

§ 3.3 El Teorema Fundamental de la Aritmética

En esta sección nos convenceremos de que los números primos son en un sentido los átomos a partir de los cuales se componen los números enteros positivos.

Número primo

Definición 3.20 (Número primo). Un *primo* es un número entero $p > 1$ cuyos únicos divisores positivos son 1 y p.

Por definición, 1 no es un número primo. Más adelante demostraremos que existen infinitos números primos (Teorema 3.24). El conjunto de los números primos es:

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots\}.$$

> ☞ **Antes de seguir leyendo**
>
> Sean $a, p, q \in \mathbb{Z}$ y supongamos que p y q son números primos. Demuestre lo siguiente:
>
> 1. Si $p \nmid a$ entonces $(a, p) = 1$.
> 2. Si $p \neq q$ entonces $p \nmid q$ y $q \nmid p$.

Los números primos tienen propiedades especiales. Por ejemplo, si un número primo divide a un producto de números enteros, entonces divide a alguno de ellos:

Lema de Euclides

Teorema 3.21 (Lema de Euclides). Si p es un número primo y $p \mid ab$, entonces $p \mid a \vee p \mid b$.

Prueba. Se deja al lector (ejercicio 1). ∎

Corolario 3.22. Si p es un número primo y $p \mid d_1 d_2 \cdots d_n$, entonces $p \mid d_i$ para algún i entre 1 y n.

Prueba. La demostración se puede hacer por medio de inducción matemática en n y se deja al lector (ejercicio 2). ∎

El teorema más importante de divisibilidad es el que le otorga a los números primos su estatus de materia prima para generar, mediante productos, todos los números naturales mayores que 1. Por ejemplo, sea $a = 72$. Intentemos factorizar a como el producto de números primos,

esto es, como un producto de la forma $q_1 q_2 \cdots q_m$, en donde cada q_i es un número primo y $q_1 \leq q_2 \leq \cdots q_m$:

$$72 = (2)(36) = (2)(2)(18) = (2)(2)(2)(9) = (2)(2)(2)(3)(3).$$

Concluimos que $72 = q_1 q_2 q_3 q_4 q_5$, en donde

$$q_1 = 2,\ q_2 = 2,\ q_3 = 2,\ q_4 = 3,\ q_5 = 3.$$

El siguiente teorema establece que este proceso siempre es posible y, además, que sólo hay una forma de hacerlo:

TFA: *Teorema Fundamental de la Aritmética*

Teorema 3.23 (Teorema Fundamental de la Aritmética, TFA). Todo número entero $n > 1$ tiene una única factorización en números primos. En otras palabras, existe $m > 0$ tal que

$$n = q_1 q_2 \cdots q_m,$$

en donde cada q_i es un número primo y $q_1 \leq q_2 \leq \cdots \leq q_m$. Además, tal factorización es única. Esto es, si n es de la forma

$$n = q_1' q_2' \cdots q_s',$$

en donde cada q_i' es un número primo y $q_1 \leq q_2 \leq \cdots \leq q_s$, entonces $m = s$ y $q_i = q_i'$ para todo i tal que $1 \leq i \leq m$.

Prueba. Utilizamos el PIF sobre n. Sea $n \in \mathbb{N}$ y supongamos que el resultado que queremos establecer es válido para todo $k \in \mathbb{N}$ tal que $1 < k < n$. Demostremos que es válido para n. Supongamos que $n > 1$. Si n es un número primo, entonces $n = n$ y tal factorización en números primos (el producto de un único número primo) es única. Si n no es un número primo, entonces por definición existen $a, b \in \mathbb{N}$, $a, b > 1$, tales que $n = ab$. Esto implica que $1 < a < n$ y $1 < b < n$, así que por hipótesis de inducción tenemos que

$$a = s_1 \cdots s_d \text{ y } b = t_1 \cdots t_e,$$

en donde los s_i y los t_i son todos números primos. Entonces

$$n = t_1 \cdots t_d s_1 \cdots s_e.$$

Si reordenamos este producto de menor a mayor, obtenemos la factorización de n en primos: $n = q_1 \cdots q_m$ $(m = d + e)$, con $q_i \leq q_{i+1}$ para $1 \leq i < m$. Cada q_i será algún s_j o t_j. Para demostrar la unicidad de la representación de n, supongamos ahora que $n = q_1' \cdots q_s'$, en donde los q_i' son números primos y $q_i' \leq q_{i+1}'$ para $1 \leq i \leq s$. Entonces

$$q_1 q_2 \cdots q_m = q_1' q_2' \cdots q_s'.$$

Note que $m, s > 1$, pues de lo contrario n sería un número primo. Como q_m divide a $q_1' q_2' \cdots q_s'$, por el Corolario 3.22 existe i tal que $q_m \mid q_i'$. Pero, como q_m y q_i' son ambos primos, $q_m = q_i' \leq q_s'$. También tenemos que q_s'

divide a $q_1 q_2 \cdots q_m$, luego existe j tal que $q'_s = q_j \leq q_m$. Por antisimetría $q_m = q'_s$, luego por la Ley Cancelativa[5] tenemos:

$$q_1 q_2 \cdots q_{m-1} = q'_1 q'_2 \cdots q'_{s-1}.$$

Tomemos $k := q_1 \cdots q_{m-1}$. Dado que $k < n$, concluimos por hipótesis de inducción que, debido a la unicidad de representación, $m - 1 = s - 1$ y $q_j = q'_j$ para todo j entre 1 y $m - 1$. Se sigue que $m = s$ y $q_j = q'_j$ para todo j entre 1 y m, como queríamos. ∎

Una consecuencia importante del TFA es la existencia de infinitos números primos. La prueba de este hecho fue dada por el matemático griego Euclides:

Teorema 3.24. Existen infinitos números primos.

Prueba. Supongamos que hay un número finito de números primos y sean todos ellos:

$$p_0, p_1, p_2, \ldots, p_r$$

(donde $r \in \mathbb{N}^*$). Sea $n = p_0 p_1 \cdots p_r + 1$. Es claro que n es mayor que cada número primo p_i. Luego n no es primo y por el TFA, existe un número primo p_j y un número entero c tal que

$$n = p_j c = p_j (p_1 p_2 \cdots p_{j-1} p_{j+1} \cdots p_r) + 1.$$

Entonces

$$p_j (c - p_1 p_2 \cdots p_{j-1} p_{j+1} \cdots p_r) = 1,$$

lo cual es imposible, pues $p_j > 1$. ∎

Vamos a construir ahora una enumeración de los números primos. Esto es, definimos recursivamente el número primo p_n así:

(a) $p_0 := 2$ (el primer número primo).

(b) $p_{i+1} :=$ "el mínimo número primo mayor que p_i". Este número p_{i+1} existe gracias al PBO y al hecho de que existen infinitos números primos.

Por ejemplo, $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, etc. Claramente, para todo $n \in \mathbb{N}$ tenemos que $p_n < p_{n+1}$. En principio podría ocurrir que existiera algún número primo p que no estuviera en nuestra enumeración, es decir, tal que para todo $n \in \mathbb{N}$, $p \neq p_n$. Como veremos, este no es el caso y la enumeración dada es *exhaustiva*, es decir, enumera a todos los números primos:

[5] En el conjunto de los números enteros, la Ley Cancelativa afirma que si $ab = a'b$ y $b \neq 0$, entonces $a = a'$.

Observación 3.25. Sea P el conjunto de los números primos. Entonces:

$$P = \{p_n : n \in \mathbb{N}\}.$$

Prueba. Definamos $R := \{p_n : n \in \mathbb{N}\} = \{p_0, p_1, p_2, \dots\}$. Debemos demostrar que $R = P$. Utilizamos el método de doble inclusión:

(⊆) Sea $p \in R$. Entonces existe $n \in \mathbb{N}$ tal que $p = p_n$. Por definición, p_n es un número primo, luego $p \in P$.

(⊇) Supongamos, buscando una contradicción, que $P \nsubseteq R$. Esto implica que $A := P \setminus R$ es un conjunto no vacío. Por el PBO, sea $q = \text{MÍN}(A)$. Entonces $q \neq 2$, pues $2 = p_0 \in R$. Ahora consideremos el conjunto $B = \{p \in \mathbb{N} : p \in R, p < q\}$. Este conjunto B es finito y no vacío y por ende, debe tener un elemento máximo, $p_n = \text{MÁX}(B)$. Entonces $p_n < q$. Veamos que $q = p_{n+1}$:

(≤) $p_n < p_{n+1}$, por maximalidad de p_n, $p_{n+1} \notin B$ y tenemos que $q \leq p_{n+1}$.

(≥) Dado que p_{n+1} es el mínimo primo mayor que p_n y, además, $p_n < q$, entonces necesariamente $q \geq p_{n+1}$.

Por antisimetría, $q = p_{n+1}$, pero entonces $q \in R$, lo cual es una contradicción. Concluimos que $P \setminus R = \varnothing$ o, equivalentemente, que $P \subseteq R$, como queríamos. ∎

Para desarrollar lo que sigue introducimos la notación de producto generalizado:

Definición 3.26 (Notación de producto generalizado). Si $a_0, a_1, \dots, a_k$ son números reales, definimos *Producto generalizado*

$$\prod_{i=0}^{k} a_i := a_0 a_1 \dots a_k,$$

y a tal número lo llamamos el *producto de los a_i, desde $i = 0$ hasta k.*[6]

Una factorización en números primos puede incluir en muchas ocasiones primos repetidos. Por ejemplo,

$$4000 = (2)(2)(2)(2)(2)(5)(5)(5) = 2^5 3^0 5^3 = p_0^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2},$$

[6] Al igual que sucede con la notación para la unión e intersección generalizadas y la sumatoria, es corriente hallar los términos del producto desplazados hacia la derecha, de esta manera: $\prod_{i=0}^{k} a_i$.

en donde $(\alpha_0, \alpha_1, \alpha_2) = (5, 0, 3)$. En notación de producto generalizado, tenemos que

$$4000 = \prod_{i=0}^{2} p_i^{\alpha_i}.$$

Teniendo en cuenta esta notación más concisa, el TFA puede ser reformulado de la siguiente manera:

Teorema 3.27 (Reformulación del TFA). Sea $n \in \mathbb{N}$. Si $n > 1$, entonces existe $k \in \mathbb{N}$ tal que

$$n = \prod_{i=0}^{k} p_i^{\alpha_i} = p_0^{\alpha_0} p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

con $\alpha_i \in \mathbb{N}$ para $0 \leq i \leq k$, y $\alpha_k > 0$. Además, esta representación es única, esto es, si

$$n = \prod_{i=0}^{s} p_i^{\beta_i},$$

con $\beta_i \in \mathbb{N}$ para $0 \leq i \leq s$ y $\beta_s > 0$, entonces $k = s$ y $\alpha_i = \beta_i$, para todo i con $0 \leq i \leq k$. Esta representación se llama la *factorización canónica de n*.

Factorización canónica

Prueba. Se sigue inmediatamente del TFA y la Definición 3.26. ∎

Ejemplo 3.28. Dados $n_0 = 36$, $n_1 = 78$ y $n_2 = 350$, exprese a cada n_s como $\prod_{i=0}^{k} p_i^{\alpha_i^s}$ (donde $s = 0, 1, 2$).

Solución. Tomamos $k = 5$.

(a) $s = 0$: $\alpha_0^0 = 2, \alpha_1^0 = 2, \alpha_2^0 = 0, \alpha_3^0 = 0, \alpha_4^0 = 0, \alpha_5^0 = 0$, de modo que $\prod_{i=0}^{5} p_i^{\alpha_i^0} = 2^2 3^2 5^0 7^0 11^0 13^0 = n_0$.

(b) $s = 1$: $\alpha_0^1 = 1, \alpha_1^1 = 1, \alpha_2^1 = 0, \alpha_3^1 = 0, \alpha_4^1 = 0, \alpha_5^1 = 1$, de modo que $\prod_{i=0}^{5} p_i^{\alpha_i^1} = 2^1 3^1 5^0 7^0 11^0 13^1 = n_1$.

(c) $s = 2$: $\alpha_0^2 = 1, \alpha_1^2 = 0, \alpha_2^2 = 2, \alpha_3^2 = 1, \alpha_4^2 = 0, \alpha_5^2 = 0$, de modo que $\prod_{i=0}^{5} p_i^{\alpha_i^2} = 2^1 3^0 5^2 7^1 11^0 13^0 = n_2$.

Este ejemplo ilustra el hecho de que, dado un número finito de números naturales positivos $n_0, \ldots, n_r$, es posible encontrar $k \in \mathbb{N}$ y números

enteros α_i^s $(0 \le i \le k,\ 0 \le s \le r)$ tales que para todo s con $0 \le s \le r$ se tenga lo siguiente:

$$n_s = \prod_{i=0}^{k} p_i^{\alpha_i^s}.$$

El TFA permite determinar si un número positivo divide a otro, al comparar sus factorizaciones canónicas:

Teorema 3.29. Sea $n = \prod_{i=0}^{k} p_i^{\alpha_i}$ un número natural positivo. Dado un número entero $d > 0$, $d \mid n$ si y sólo si d es de la forma $d = \prod_{i=0}^{k} p_i^{\beta_i}$, con $0 \le \beta_i \le \alpha_i$ para todo i entre 0 y k.

Prueba. Utilizamos el método de doble implicación:

(→) Sea $c > 0$ tal que $cd = n$. Todo número primo que divide a c o que divide a d debe dividir a n. Por ende, por el TFA, tenemos que

$$c = \prod_{i=0}^{k} p_i^{\sigma_i},\ d = \prod_{i=0}^{k} p_i^{\beta_i},\ \text{con } \sigma_i + \beta_i = \alpha_i, \sigma_i, \beta_i \ge 0.$$

Concluimos que $0 \le \beta_i \le \alpha_i$, para todo i entre 0 y k.

(←) Dado i entre 0 y k, sea $\sigma_i = \alpha_i - \beta_i$. Por hipótesis $\beta_i \le \alpha_i$, luego $\sigma_i \ge 0$ y, por ende, $c = \prod_{i=0}^{k} p_i^{\sigma_i}$ es en efecto un número natural. Dado que $d > 0$ y $cd = n$, concluimos que $d \mid n$. ∎

Como corolario obtenemos una elegante caracterización del máximo común divisor entre dos números enteros:

Corolario 3.30. Sean $a = \prod_{i=0}^{k} p_i^{\alpha_i}$ y $b = \prod_{i=0}^{k} p_i^{\beta_i}$ dos números enteros positivos y sea $d = \prod_{i=0}^{k} p_i^{m_i}$, donde $m_i = \text{MÍN}(\alpha_i, \beta_i))$.[7] Entonces $d = (a, b)$.

Prueba. El hecho de que $d \mid a$ y $d \mid b$ es una consecuencia del Teorema 3.29, pues para todo i se tiene que $m_i \le \alpha_i, \beta_i$. Además, si e es un divisor positivo de a y b, entonces e es de la forma $\prod_{i=0}^{k} p_i^{r_i}$ con $r_i \le \alpha_i, \beta_i$, así que

[7] Por definición, dados $a, b \in \mathbb{R}$, $\text{MÍN}(a, b)$ es el mínimo entre a y b; en otras palabras, $\text{MÍN}(a, b) := \text{MÍN}(X)$, donde $X = \{a, b\}$.

$r_i \leq m_i$ y por tanto $e \mid d$ (utilizando de nuevo el teorema anterior). Gracias al Teorema 3.13, concluimos que $d = (a,b)$. ∎

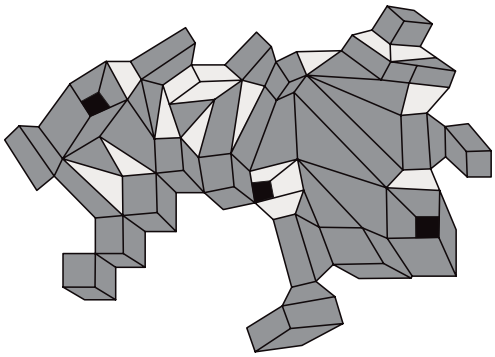
Ejemplo 3.31. Estos son algunos ejemplos de cómo calcular (a,b) utilizando el Corolario 3.30:

(a) Sean $a = 36$ y $b = 24$. Entonces $a = 2^2 3^2$ y $b = 2^3 3^1$. Se tiene entonces que $(a,b) = 2^2 3^1 = 12$.

(b) Sean $a = 405$ y $b = 1800$. Entonces $a = 2^0 3^4 5^1$ y $b = 2^3 3^2 5^2$. Se tiene entonces que $(a,b) = 2^0 3^2 5^1 = 15$.

(c) Si $a = 3^2 5^1 7^3 = 2^0 3^2 5^1 7^3 11^0$ y $b = 2^3 7^2 11^1 = 2^3 3^0 5^0 7^2 11^1$, entonces $(a,b) = 2^0 3^0 5^0 7^2 11^0 = 7^2$.

Ejercicios



1. Demuestre el Lema de Euclides (Teorema 3.21). (*Ayuda*: utilice el Teorema 3.19.)
2. Demuestre el Corolario 3.22.
3. Mediante la caracterización del MCD según el TFA (Corolario 3.30), demuestre las siguientes propiedades del MCD (donde $a,b,m \in \mathbb{N}^*$):
   (a) *Conmutatividad*: $(a,b) = (b,a)$.
   (b) *Distributividad*: $(ma,mb) = m(a,b)$.
   (c) *Asociatividad*: $((a,b),c) = (a,(b,c))$.
   (d) *Absorción*: $(a,(a,b)) = (a,b)$.

4. Mediante la caracterización del MCD según el TFA, demuestre las siguientes afirmaciones:
   (a) Si $(a,x) = d$ y $(b,x) = 1$, entonces $(ab,x) = d$.
   (b) Si $a \mid c$ y $b \mid c$, entonces $\frac{ab}{(a,b)} \mid c$.
   (c) Si $(a,x) = (b,x) = 1$, entonces $(ab,x) = 1$.
   (d) Si $(a,x) = 1$ y $a \mid xy$, entonces $a \mid y$.
5. Demuestre que para todo $n \in \mathbb{N}^*$, si $b = 2^n$, entonces $2^b - 1$ es el producto de n o más números primos.
6. Sean $n, m \in \mathbb{N}^*$. Demuestre las siguientes afirmaciones:
   (a) Si $m^2 = kn^2$, con $k \in \mathbb{N}$, entonces k es un cuadrado perfecto, esto es, existe $c \in \mathbb{N}$, tal que $k = c^2$.
   (b) $n \mid m$ si y solamente si $n^2 \mid m^2$.
7. Demuestre que si $n \geq 2$ y n no es un número primo, entonces existe un número primo p tal que $p \mid n$ y $p^2 \leq n$.
8. Dado $a \in \mathbb{Z}$, sea P_a el conjunto de todos los números primos que dividen a a.
   (a) Demuestre que dados $a, b \in \mathbb{Z}$, $(a,b) = 1 \leftrightarrow P_a \cap P_b = \varnothing$.
   (b) Demuestre que dados $a, b \in \mathbb{Z}$, $P_{ab} = P_a \cup P_b$.
   (c) Si $a \in \mathbb{Z}$ y $n \in \mathbb{N}^*$, calcule el conjunto P_{a^n} en términos de P_a.
   (d) Compare las afirmaciones "$a \mid b$" y "$P_a \subseteq P_b$": ¿son equivalentes, alguna implica a la otra o no son comparables? Justifique claramente su respuesta.
9. Demuestre que para todo $n > 1$ existen n números naturales consecutivos que no son primos (esto da una idea de la distribución irregular de los números primos). (*Ayuda*: considere los números $(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$.)
10. Demuestre que para todo número primo p, $((p-1)!, p) = 1$.
11. Demuestre que si n y m son primos relativos, con $n, m > 0$ y $nm = a^k$ para algún $k \in \mathbb{N}^*$, entonces existen $x, y \in \mathbb{Z}$ tales que $n = x^k$ y $m = y^k$.
12. Sean $a, b \in \mathbb{N}^*$ y sea $d = (a,b)$, con $a = dx$ y $b = dy$. Demuestre que $(x,y) = 1$, utilizando la caracterización del MCD según el TFA.
13. Sean $a, b, n \in \mathbb{N}^*$. Demuestre que $(a^n, b^n) = (a,b)^n$.

§ 3.4 Sucesiones finalmente nulas y el TFA

A-sucesión

Definición 3.32 (Sucesión). Sea A un conjunto cualquiera. Definimos una *A-sucesión* como una función[8] $a : \mathbb{N} \to A$. Por ende, la función a le asigna a cada número natural i un elemento $a_i \in A$. Diremos que a es una *sucesión* si existe un conjunto A tal que a es una A-sucesión.

Sucesión

Tupla infinita

A cada A-sucesión a la podemos representar como una *tupla infinita*, en donde los valores de la función a aparecen de forma ordenada:

$$a = (a_0, a_1, a_2, \dots).$$

Por ejemplo, la $\mathbb{R}$-sucesión h, dada por $h_i = 1 - i^2$, se encuentra representada por la siguiente tupla infinita:

$$\begin{aligned} h &= (h_0, h_1, h_2, h_3, h_4, \dots) \\ &= (1, 0, -3, -8, -15, \dots). \end{aligned}$$

Una notación intensional para esta tupla es $h = (h_i)_{i\in\mathbb{N}} = (1 - i^2)_{i\in\mathbb{N}}$.

Sucesión finalmente nula

Definición 3.33. Si a es una sucesión, $a = (a_i)_{i\in\mathbb{N}}$, diremos que a es *finalmente nula* si existe $N \in \mathbb{N}$ tal que para todo $i \in \mathbb{N}$ con $i \geq N$ se tiene que $a_i = 0$. Formalmente, a es una sucesión finalmente nula si y sólo si

$$\exists N \in \mathbb{N} : \forall i \in \mathbb{N}, i \geq N \to a_i = 0.$$

Sea $\mathcal{F}$ el conjunto de todas las $\mathbb{N}$-sucesiones que son *finalmente nulas*, esto es,

$$\mathcal{F} = \{ (a_i)_{i\in\mathbb{N}} : a \text{ es una } \mathbb{N}\text{-sucesión y } a \text{ es finalmente nula} \}.$$

Por ejemplo, la $\mathbb{N}$-sucesión v dada por $v_i = \max(0, 8 - 3i)$,[9] se puede representar por la tupla infinita

$$\begin{aligned} v &= (v_0, v_1, v_2, v_3, v_4, v_5, v_6, \dots) \\ &= (8, 5, 2, 0, 0, 0, 0, \dots). \end{aligned}$$

Es claro que para todo $i \geq 3$, $v_i = 0$, luego v es finalmente nula y $v \in \mathcal{F}$. Por otro lado, si w es la $\mathbb{N}$-sucesión dada por $w_i = (-1)^i + 1$, entonces

$$w = (2, 0, 2, 0, \dots).$$

Esta sucesión w no es finalmente nula, puesto que los valores de w tomarán infinitos valores distintos de 0. Luego $w \notin \mathcal{F}$.

---

[8] El concepto de función será definido en detalle en la § 4.3.

[9] Simbolizamos el máximo entre a y b como $\max(a, b)$.

☞ **Antes de seguir leyendo**

Sean a y b $\mathbb{N}$-sucesiones, y $\mathcal{F}$ el conjunto de todas las $\mathbb{N}$-sucesiones que son finalmente nulas.

1. Demuestre que $a \in \mathcal{F}$ si y sólo si el conjunto $\{i \in \mathbb{N} : a_i \neq 0\}$ es finito.
2. Imaginemos que una $\mathbb{N}$-sucesión a es un computador infinito que puede guardar en su memoria ordenada los números naturales $a_0, a_1, a_2, \ldots$, y que $a_i = 0$ significa que el espacio i-ésimo en memoria no es utilizado por el computador. Por ejemplo, la tupla constante 0, es decir, $(0, 0, 0, \ldots)$, representa el "computador sin memoria". De acuerdo con esta analogía, ¿cómo describiría al conjunto $\mathcal{F}$?
3. Definimos la suma de dos $\mathbb{N}$-sucesiones a y b, $a + b$, como la $\mathbb{N}$-sucesión c tal que $c_i = a_i + b_i$, esto es, la suma *componente por componente*. Por ejemplo, si $a = (i + 2)_{i \in \mathbb{N}}$ y $b = (3i - 1)_{i \in \mathbb{N}}$, entonces $a + b = (4i + 1)_{i \in \mathbb{N}}$. Demuestre que si $a, b \in \mathcal{F}$, entonces $a + b \in \mathcal{F}$.
4. Sean a una $\mathbb{N}$-sucesión y $n \in \mathbb{N}$. Definimos na como la $\mathbb{N}$-sucesión c tal que $c_i = na_i$ Por ejemplo, si $a = (3i + 2)_{i \in \mathbb{N}}$ y $n = 4$, entonces $na = (12i + 8)_{i \in \mathbb{N}}$. Demuestre que si $a \in \mathcal{F}$ y $n \in \mathbb{N}$, entonces $na \in \mathcal{F}$.
5. Sea a la $\mathbb{R}$-sucesión dada por $a_i = \frac{1}{1+i}$. ¿Es a finalmente nula? Justifique su respuesta.

El TFA establece una conexión fuerte entre los conjuntos $\mathbb{N}^*$ y $\mathcal{F}$: todo número natural positivo

$$n = \prod_{i=0}^{m} p_i^{\alpha_i}$$

está asociado de un modo bien definido, esto es gracias a la unicidad de representación, con la sucesión finalmente nula

$$n_{()} = (\alpha_0, \alpha_1, \ldots, \alpha_m, 0, 0, 0, \ldots) \in \mathcal{F}.$$

Recíprocamente, toda tupla $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_m, 0, 0, 0, \ldots) \in \mathcal{F}$ está asociada con el número natural positivo $\pi(\alpha)$ dado por

$$\pi(\alpha) = \prod_{i=0}^{m} p_i^{\alpha_i} \in \mathbb{N}^*.$$

Aquí utilizamos el hecho de que existen infinitos números primos p_0, p_1, p_2, … En particular, la tupla $(0, 0, 0, \ldots) \in \mathcal{F}$ se encuentra asociada con el número natural $2^0 = 1$.

Veamos que $_{()}$ y π son operaciones *inversas entre sí*, es decir, para todo $n \in \mathbb{N}^*$ y para todo $v \in \mathcal{F}$, $(\pi(v))_{()} = v$ y $\pi(n_{()}) = n$:

(a) Dada $v = (a_i)_{i\in\mathbb{N}} \in \mathcal{F}$, $\pi(v)$ es el número natural cuya *única* factorización en números primos es

$$\prod_{i=0}^{m} p_i^{a_i},$$

donde m es el máximo natural i tal que $a_i \neq 0$ (o $m = 0$, si todos los a_i son 0). Por definición de $_{()}$, esto es equivalente a afirmar que $(\pi(v))_{()}$ es igual a v.

(b) Dado $n = \prod_{i=0}^{m} p_i^{a_i} \in \mathbb{N}^*$, entonces $n_{()} = (a_i)_{i\in\mathbb{N}}$, donde $a_i = 0$ para $i > m$; por eso, $\pi(n_{()}) = \prod_{i=0}^{m} p_i^{a_i} = n$.

Ejemplo 3.34. Algunas representaciones de enteros positivos como elementos de $\mathcal{F}$. Aquí escribimos $n \sim n_{()}$ o, lo que es lo mismo, $\pi(v) \sim v$:

(a) $1 \sim (0,0,0,0,0,0,0,\dots)$.
(b) $2 \sim (1,0,0,0,0,0,0,\dots)$.
(c) $6 \sim (1,1,0,0,0,0,0,\dots)$.
(d) $11 \sim (0,0,0,0,1,0,0,\dots)$.
(e) $28 \sim (2,0,0,1,0,0,0,\dots)$.
(f) $36 \sim (2,2,0,0,0,0,0,\dots)$.
(g) $64 \sim (6,0,0,0,0,0,0,\dots)$.
(h) $98 \sim (1,0,0,2,0,0,0,\dots)$.
(i) $120 \sim (3,1,1,0,0,0,0,\dots)$.
(j) $210 \sim (1,1,1,1,0,0,0,\dots)$.
(k) $19^4 \sim (0,0,0,0,0,0,0,4,0,0,0,\dots)$.
(l) $7927 \sim (a_i)_{i\in\mathbb{N}}$, donde $a_{1000} = 1$ y $a_i = 0$ para $i \neq 1000$.

En resumen, hemos identificado a $\mathbb{N}^*$ con $\mathcal{F}$. Pero podemos hacer más; definimos el siguiente orden $\leq$ en el conjunto $\mathcal{F}$:

$$(a_i)_{i\in\mathbb{N}} \leq (b_i)_{i\in\mathbb{N}} \text{ si y sólo si, para todo } i \in \mathbb{N}, a_i \leq b_i.$$

Esto es, una sucesión finalmente nula es menor o igual a otra si es menor o igual *componente por componente*. Por ejemplo,

$$(2,3,5,0,12,0,0,\dots) \leq (4,3,9,0,13,3,0,0,\dots).$$

La sucesión finalmente nula $(0,0,0,\dots)$ es el elemento mínimo de $\mathcal{F}$. Es fácil verificar que el nuevo orden definido es un orden parcial. Más aún:

Teorema 3.35. $(\mathcal{F},\leq) \cong (\mathbb{N}^*,|)$.[10]

Prueba. Sea $\pi : \mathcal{F} \to \mathbb{N}^*$ la función definida atrás. Para todo $n \in \mathbb{N}^*$ existe un único $v \in F$ tal que $\pi(v) = n$. Basta tomar $v = n_{()}$ y entonces se tiene que $\pi(v) = \pi(n_{()}) = n$). Es único pues si tenemos $w \in \mathcal{F}$ tal que $\pi(w) = n$, entonces $w = (\pi(w))_{()} = n_{()} = v$. Ahora bien, el hecho de que $a = (a_i)_{i\in\mathbb{N}} \leq (b_i)_{i\in\mathbb{N}} = b$, si y sólo si $\pi(a) \mid \pi(b)$, es una consecuencia inmediata del Teorema 3.29. Por ende, π es un homomorfismo entre órdenes. ∎

Ejemplo 3.36. Calcule el número de divisores positivos de 80.

Solución. Sabemos que $80 = 2^4 3^0 5^1$, luego $80_{()} = (4,0,1,0,0,\dots)$. Un divisor positivo de 80 es un número $m \in \mathbb{N}^*$ tal que $m \mid 80$, lo que es equivalente (gracias al Teorema 3.35) a decir que $m_{()} \leq 80_{()}$. Entonces para contar a los divisores positivos de 80, basta contar todas las tuplas $(a_0,a_1,a_2,0,0,\dots) \in \mathcal{F}$ tales que

$$(a_0,a_1,a_2,0,0,\dots) \leq (4,0,1,0,0,\dots).$$

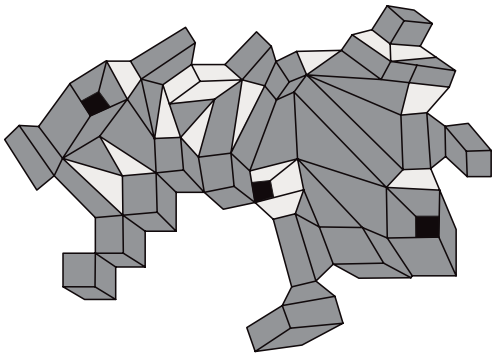
Entonces $0 \leq a_0 \leq 4$, $a_1 = 0$ y $0 \leq a_2 \leq 1$. Así, a_0 tiene cinco posibilidades, a_1 tiene una posibilidad y a_2 tiene dos posibilidades. Si multiplicamos estas posibilidades concluimos que existen exactamente $(5)(1)(2) = 10$ tuplas $v \in \mathcal{F}$ menores o iguales que $(4,0,1,0,0,\dots)$ y por ende, existen exactamente 10 divisores positivos de 80. Por ejemplo, si $v = (3,0,1,0,0,\dots)$, se tiene entonces que $v \leq 80_{()}$ y $\pi(v) = 2^3 3^0 5^1 = 40$. Claramente $40 \mid 80$.

☞ **Antes de seguir leyendo**

1. Calcule el número de divisores positivos de 594.
2. Liste todos los elementos del conjunto $\{v \in \mathcal{F} : \pi(v) \mid 36\}$.
3. Demuestre que para todo $k \in \mathbb{N}^*$ existe $n \in \mathbb{N}^*$ tal que n tiene exactamente k divisores positivos.

[10] Véase la § 2.4 para la definición de estructuras ordenadas isomorfas.

Ejercicios



1. Calcule el número de divisores positivos de los siguientes números:

   (a) 2940, (b) 1000000, (c) $2^5 15^7$.

2. Sea $n \in \mathbb{N}$. Demuestre que si $n = p_0 p_1 \cdots p_k$, entonces se tiene que $(D_n^+, |) \cong (\mathcal{P}(\{0,1 \ldots k\}), \subseteq)$. (Recuerde que p_i es el $(i+1)$-ésimo primo. Véase la § 2.4 para el concepto de isomorfismo entre estructuras ordenadas.)

3. Sea $n_{()}$ la función definida en la sección 3.4. Sean $a, b, n \in \mathbb{N}$.

   (a) Calcule $4680_{()}$.

   (b) Calcule $((4680)(121)19^4)_{()}$.

4. Sea π la función definida en la sección 3.4. Sean $a, b, n \in \mathbb{N}$.

   (a) Dé una descripción de $\pi(a^n)$ en términos de $\pi(a)$ y n.

   (b) Dé una descripción de $\pi(ab)$ en términos de $\pi(a)$ y $\pi(b)$.

5. Demuestre que para todo $n \in \mathbb{N}^*$, si un número $a \in \mathbb{N}$ tiene por lo menos n divisores primos distintos, entonces a tiene por lo menos 2^n divisores positivos distintos.

6. Sea $n \in \mathbb{N}^*$ y suponga que n tiene un número impar de divisores positivos. Demuestre que para todo número primo p, si $p \mid n$ entonces $p^2 \mid n$.

7. Sea $n \in \mathbb{N}^*$. Demuestre que si n tiene un número primo de divisores positivos, entonces n es la potencia positiva de un primo (es decir, existe $k \in \mathbb{N}^*$ y un número primo p tal que $n = p^k$).

8. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:

(a) Para todo $k \in \mathbb{N}^*, (k\mathbb{N}, |) \cong (\mathbb{N}, \leq)$. (Tenga en cuenta que por definición $k\mathbb{N} = \{kn : n \in \mathbb{N}\} = \{0, k, 2k, 3k, \dots\}$.)

(b) Para todo $k \in \mathbb{N}$ con $k > 1$, $(\{k^i : i \in \mathbb{N}\}, |) \cong (\mathbb{N}, \leq)$.

(c) Para todo $k \in \mathbb{N}^*$, $(k\mathbb{N}, |) \cong (\mathbb{N}^*, |)$.

(d) Para todo $k \in \mathbb{N}^*$, $(k\mathbb{N}^*, |) \cong (\mathbb{N}^*, |)$.

9. Usted se encuentra en el centro de un enorme cuarto que tiene 100 puertas numeradas del 1 al 100, todas las cuales se encuentran cerradas inicialmente. Un mago que se encuentra a su lado comienza a pronunciar lentamente los números del 1 al 100, en orden ascendente. Cada vez que el mago pronuncia el número i, las puertas que son múltiplos de i cambian mágicamente de estado, esto es, se cierran si estaban abiertas, y se abren si estaban cerradas. Cuando el mago haya terminado de pronunciar el número 100, ¿exactamente qué puertas habrán quedado abiertas?

10. Para este ejercicio considere la siguiente definición:

Definición (mínimo común múltiplo, MCM). Dado $a \in \mathbb{Z}$, definimos $(a) := \{ka : a \in \mathbb{Z}\}$. Dados $a, b \in \mathbb{Z}$, no ambos nulos, definimos el *mínimo común múltiplo* entre a y b como

$$\text{MCM}(a, b) := \text{MÍN}((a)^+ \cap (b)^+).$$

(a) Demuestre que $m = \text{MCM}(a, b)$ verifica que $a \mid m$, $b \mid m$, y si e es múltiplo de a y b, entonces $m \mid e$.

(b) Demuestre que la operación MCM es conmutativa y asociativa.

(c) Demuestre que $(a, b) = 1$ si y sólo si $\text{MCM}(a, b) = |ab|$.

(d) Para $a, b \in \mathbb{N}^*$, dé una caracterización de la factorización en primos de $\text{MCM}(a, b)$ en términos de las factorizaciones en primos de a y b.

11. Mediante la caracterización del MCM según el TFA, demuestre las siguientes propiedades relativas al MCD (donde $a, b, c, k \in \mathbb{N}^*$):

(a) *Conmutatividad*: $\text{MCM}(a, b) = \text{MCM}(b, a)$.

(b) *Distributividad*: $\text{MCM}(ka, kb) = k \cdot \text{MCM}(a, b)$.

(c) *Asociatividad*: $\text{MCM}(\text{MCM}(a, b), c) = \text{MCM}(a, \text{MCM}(b, c))$.

(d) *Absorción*: $\text{MCM}(a, \text{MCM}(a, b)) = \text{MCM}(a, b)$.

12. Utilizando la caracterización del MCM según el TFA, demuestre que, dados $a, b, c \in \mathbb{N}^*$, si $c \mid a$ y $c \mid b$, entonces $c \mid d$, donde d es el número dado por $d = \frac{ab}{\text{MCM}(a,b)}$.

§ 3.5 Congruencias y el Pequeño Teorema de Fermat

En esta sección consideraremos un número natural positivo n y con base en él clasificaremos todos los números enteros según cuáles sean sus residuos al dividirlos por n. El siguiente ejemplo ilustra esto:

Ejemplo 3.37. Sea $n = 3$. Sabemos que al dividir un número entero x por 3, hay tres posibles residuos: $r = 0$, $r = 1$ y $r = 2$. Esto es, para todo x existen dos enteros únicos q y r tales que $x = 3q + r$, con $0 \leq r < 3$, lo que permite clasificar todos los números enteros en los siguientes tres conjuntos:

(a) $\{3q : q \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$. Este es el conjunto de múltiplos de 3.

(b) $\{3q + 1 : q \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$.

(c) $\{3q + 2 : q \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Es fácil ver que todo número entero x se encuentra en uno y sólo uno de los tres conjuntos anteriores.

Recordemos que dado $x \in \mathbb{Z}$, $\text{RES}_n(x)$ es el residuo que resulta de dividir a x por n, esto es,

$$r = \text{RES}_n(x) \leftrightarrow \exists q \in \mathbb{Z} : x = qn + r, \quad 0 \leq r < n.$$

Ahora introducimos la relación de *congruencia módulo n* sobre $\mathbb{Z}$:

$\equiv_n$: *Congruencia módulo n.*

Definición 3.38. Sea n un número natural positivo. Sean x y y números enteros. Diremos que x y y son *congruentes módulo n* (lo que se simboliza así: $x \equiv_n y$), si $\text{RES}_n(x) = \text{RES}_n(y)$.

Ejemplo 3.39. Veamos algunos ejemplos de la relación de congruencia módulo n:

(a) $5 \equiv_4 13$; (b) $6 \not\equiv_3 10$; (c) $13 \equiv_3 -2$.

☞ **Antes de seguir leyendo**

Demuestre que, para todo $n \in \mathbb{N}$ y para todo $a \in \mathbb{Z}$, $a \equiv_n a + n$.

Teorema 3.40. Sea $n \in \mathbb{N}^*$. La relación de congruencia módulo n cumple con las siguientes propiedades:

(a) *reflexividad*: dado $x \in \mathbb{Z}$, $x \equiv_n x$;

(b) *simetría*: dados $x, y \in \mathbb{Z}$, si $x \equiv_n y$, entonces $y \equiv_n x$;

(c) *transitividad*: dados x, y, $z \in \mathbb{Z}$, si $x \equiv_n y$ y, además, $y \equiv_n z$, entonces $x \equiv_n z$.

Prueba. La demostración es evidente. ∎

El siguiente teorema caracteriza, en términos de la divisibilidad, la relación de congruencia módulo n y será utilizado ampliamente durante esta sección:

Teorema 3.41. Dados $n \in \mathbb{N}^*$ y $x, y \in \mathbb{Z}$, $x \equiv_n y$ si y sólo si la diferencia entre x y y es divisible por n, es decir, si $n \mid (y - x)$.

Prueba. Utilizamos el método de doble implicación:

(→) Supongamos que $x \equiv_n y$. Esto significa que $\text{RES}_n(x) = \text{RES}_n(y) = r$. Sabemos que existen $q_1, q_2 \in \mathbb{Z}$ tales que $x = q_1 n + r$, y $y = q_2 n + r$. Si restamos estas dos igualdades, obtenemos que $y - x = (q_2 - q_1)n$, lo cual implica que n divide a $y - x$.

(←) Supongamos que $n \mid y - x$. Entonces existe $k \in \mathbb{Z}$ tal que $y - x = kn$. Ahora, sean $x = q_1 n + r_1$, $y = q_2 n + r_2$, con $0 \leq r_1, r_2 < n$. A partir de las anteriores ecuaciones concluimos que

$$kn = y - x = (q_2 - q_1)n + r_2 - r_1,$$

lo cual implica que

$$(k - q_2 + q_1)n = r_2 - r_1.$$

Claramente $(k - q_2 + q_1)n$ no pertenece al conjunto $\{x \in \mathbb{Z} : |x| < n\}$, a menos que sea igual a 0. El número entero $r_2 - r_1$ necesariamente pertenece al conjunto $\{x \in \mathbb{Z} : |x| < n\}$, ya que $0 \leq r_1, r_2 < n$. Esto implica que $r_2 - r_1 = 0$, luego $\text{RES}_n(x) = \text{RES}_n(y)$. Así, $x \equiv_n y$. ∎

☞ **Antes de seguir leyendo**

Sea $n \in \mathbb{N}^*$. Demuestre las siguientes afirmaciones:

1. Todo número entero es congruente con su residuo. Más precisamente, para todo $x \in \mathbb{Z}$, si $r = \text{RES}_n(x)$, entonces $x \equiv_n r$.
2. $n \equiv_n 0$.
3. Para todo $x \in \mathbb{Z}$, x es múltiplo de n si y sólo si $x \equiv_n 0$.

Sabemos que 3 y 7 son congruentes módulo 4. Si multiplicamos a ambos números por 5 obtenemos $5(3) = 15$ y $5(7) = 35$, que a su vez son congruentes módulo 4. Este fenómeno no es una casualidad. El siguiente teorema establece que las congruencias entre dos números se mantienen al transformarlos a ambos de ciertas maneras.

Preservación de congruencias

Teorema 3.42 (Preservación de congruencias). Sean $a, a', b, b', s, t \in \mathbb{Z}$ y sean n, k números naturales positivos. Si $a \equiv_n a'$ y $b \equiv_n b'$, entonces:

(a) $a + s \equiv_n a' + s$ (suma de un número entero);
(b) $sa \equiv_n sa'$ (multiplicación por un número entero);
(c) $sa + tb \equiv_n sa' + tb'$ (combinación lineal);
(d) $a + b \equiv_n a' + b'$ (suma);
(e) $ab \equiv_n a'b'$ (multiplicación);
(f) $(a)^k \equiv_n (a')^k$ (exponenciación).

Prueba. Por hipótesis, y en virtud del Teorema 3.41, existen los números enteros q_1 y q_2 tales que $a' - a = q_1 n$ y $b - b' = q_2 n$.

(a) $(a' + s) - (a + s) = a' - a = q_1 n$. Luego $a + s \equiv_n a' + s$.
(b) $sa' - sa = s(a' - a) = sq_1 n$.
(c) $(sa' + tb') - (sa + tb) = s(a - a') + t(b' - b) = sq_1 n + tq_2 n = (sq_1 + tq_2)n$.
(d) Es un caso especial de (c).
(e) $a'b' - ab = (a' - a)b' + a(b' - b) = q_1 nb' + aq_2 n = (q_1 b' + aq_2)n$.
(f) Se demuestra fácilmente por inducción en k. Para el paso inductivo se utiliza (e). ∎

Polinomio

Un *polinomio* es una expresión de la forma

$$p(x) = a_0 + a_1 x + a_2 x^2 \cdots + a_k x^k,$$

en donde $a_0, a_1, \ldots, a_k \in \mathbb{Z}$. Estos números enteros son llamados los *coeficientes*[11] del polinomio $p(x)$.

Por ejemplo, $p(x) = 5 - 3x + x^2$ es un polinomio. Podemos "evaluar" el polinomio en un número entero cualquiera, por ejemplo, 2, obteniendo:

$$x = 2 \to p(x) = p(2) = 5 - 3(2) + 2^2 = 3.$$

La afirmación $p(2) = 3$ se lee de la siguiente manera: *el polinomio* $p(x)$ *evaluado en* $x = 2$ *da como resultado el valor de* 3.

Ahora bien, resulta que las congruencias entre enteros se preservan bajo la aplicación de un polinomio con coeficientes enteros:

[11] En este capítulo sólo consideraremos polinomios con coeficientes enteros. Sin embargo, en varias áreas de las matemáticas suele trabajase con polinomios más generales, cuyos coeficientes son números reales o complejos.

Corolario 3.43. Sean $n \in \mathbb{N}^*$, $a, a' \in \mathbb{Z}$, y $p(x)$ un polinomio. Si $a \equiv_n a'$, entonces $p(a) \equiv_n p(a')$.

Prueba. Se deduce fácilmente del Teorema 3.42, ya que un polinomio con coeficientes enteros se construye a partir de las operaciones mencionadas en tal teorema. ∎

En general, es fácil ver que el recíproco[12] del Teorema 3.42 (b) no es válido. Sin embargo, suponiendo cierta condición especial, obtenemos una Ley Cancelativa para las Congruencias:

Ley Cancelativa para Congruencias

Teorema 3.44 (Ley Cancelativa para las Congruencias). Sean $s, a, a' \in \mathbb{Z}$ y supongamos que $sa \equiv_n sa'$ y, además, $(s, n) = 1$. Entonces $a \equiv_n a'$.

Prueba. Por hipótesis existe $q \in \mathbb{Z}$ tal que $s(a' - a) = qn$. Esto implica que $n \mid s(a' - a)$, pero como $(s, n) = 1$, por el Teorema 3.19 concluimos que $n \mid (a' - a)$, como queríamos demostrar. ∎

Este teorema puede ser generalizado así:

Teorema 3.45. Supongamos que $sa \equiv_n sa'$ y sea $d = (s, n)$. Se tiene entonces que $a \equiv_{\frac{n}{d}} a'$.

Prueba. Se deja al lector (ejercicio 8). ∎

$\mathbb{Z}_n$: LA ESTRUCTURA DE LOS NÚMEROS ENTEROS MÓDULO n

$[x]_n$: Clase de congruencia

Definición 3.46 (Clase de congruencia). Dado $n \in \mathbb{N}^*$ y $x \in \mathbb{Z}$, definimos la *clase de congruencia de x módulo n* como el conjunto $[x]_n$ dado por:

$$[x]_n := \{y \in \mathbb{Z} : x \equiv_n y\}.$$

Dicho de otra forma, $[x]_n = \{y \in \mathbb{Z} : \text{RES}_n(x) = \text{RES}_n(y)\}$. Ahora, si $r = \text{RES}_n(x)$, entonces $[x]_n = [r]_n$. Como $0 \leq r < n$, existen exactamente n clases de congruencia módulo n:

$$[0]_n, [1]_n, \ldots, [n-1]_n.$$

Estas consideraciones nos permiten reformular el ejemplo 3.37, considerado antes:

[12] En términos lógicos, el recíproco de $p \to q$ es $q \to p$.

Ejemplo 3.47. Sea $n = 3$. Calculemos, por ejemplo, la clase de congruencia del entero $x = 8$ (módulo n). Es fácil ver que los números congruentes con 8 son los siguientes:

$$\ldots, -1, 2, 5, 8, 11, 14, 17, \ldots$$

Por ende,

$$[8]_3 = \{\ldots, -1, 2, 5, 8, 11, 14, 17, \ldots\}.$$

Ahora, $2 = \text{RES}_3(8)$ y por ende, $[8]_3 = [2]_3$. En general, al dividir un número entero x por 3, hay tres posibles residuos: $r = 0$, $r = 1$ y $r = 2$. Esto permite clasificar a los números enteros en los siguientes tres conjuntos:

(a) El conjunto de todos los números enteros congruentes con 0: $[0]_3 = \{3q : q \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$, es decir, el conjunto de múltiplos de 3,

(b) El conjunto de todos los números enteros congruentes con 1: $[1]_3 = \{3q + 1 : q \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$, y

(c) El conjunto de todos los números enteros congruentes con 2: $[2]_3 = \{3q + 2 : q \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Es fácil ver que todo número entero x se encuentra en *exactamente* uno de los tres conjuntos anteriores. Es decir,

$$\mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3;$$

además, $[0]_3, [1]_3$ y $[2]_3$ son conjuntos disjuntos entre sí. Por ejemplo, dado que $5 \not\equiv_3 10$, podemos afirmar que $[5]_3 \neq [10]_3$ y de hecho que $[5]_3 \cap [10]_3 = \varnothing$.

El siguiente ejemplo tiene como fin ilustrar la utilidad de las clases de congruencia:

Ejemplo 3.48. Considere la figura de la página siguiente. El punto que aparece en ella puede rotarse, de forma positiva o negativa, cualquier número de unidades. Más precisamente, cada número entero x representará la operación de rotar al punto un número x de unidades hacia la derecha o hacia la izquierda, respectivamente, según sea el signo de x. En principio hemos definido un número *infinito* de operaciones, una por cada número entero. Sin embargo, es claro que muchas operaciones son *equivalentes* entre sí, en el sentido de que producen el mismo resultado, esto es, mueven el punto a la misma

casilla. Dado que en general rotar $6q$ unidades es esencialmente no haber realizado ningún movimiento, podemos concluir que los números x y $r = \text{RES}_6(x)$ representan operaciones equivalentes. Concluimos que existen 6 operaciones esencialmente distintas: $0, 1, 2, 3, 4$ y 5. Por ejemplo, la operación 13 es equivalente a la operación 1 y la operación -4 es equivalente a la operación 2. Esto es, hemos logrado partir las infinitas operaciones $(\ldots, -3, -2, -1, 0, 1, 2, \ldots)$ en los siguientes seis conjuntos:

(a) $[0]_6 = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$,
(b) $[1]_6 = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$,
(c) $[2]_6 = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$,
(d) $[3]_6 = \{\ldots, -9, -3, 3, 9, 15, \ldots\}$,
(e) $[4]_6 = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$, y
(f) $[5]_6 = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$.

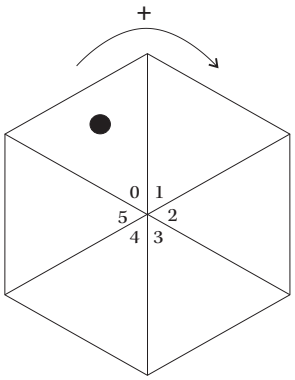


Figura 3.1 : Rotaciones de un punto en un hexágono.

Sea $n \in \mathbb{N}^*$. Consideremos el conjunto de *todas* las clases de congruencia módulo n:

$$\{[a]_n : a \in \mathbb{Z}\}.$$

Para todo número entero a se tiene que $[a]_n = [r]_n$ en donde $r = \text{RES}_n(a)$ y $0 \leq r < n$. Por esta observación concluimos que el conjunto anterior es finito y que

$$\{[a]_n : a \in \mathbb{Z}\} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

Definición 3.49. Dado un número natural positivo n, sea $\mathbb{Z}_n$ el siguiente conjunto:

$$\mathbb{Z}_n := \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

$\mathbb{Z}_n$: Enteros módulo n

A $\mathbb{Z}_n$ lo llamaremos el *conjunto de los enteros módulo n*.[13] En otras palabras, $\mathbb{Z}_n$ es el conjunto cuyos elementos son precisamente las n clases de congruencia módulo n.

En el ejemplo anterior, $\mathbb{Z}$ representa todas las operaciones de rotación, mientras que $\mathbb{Z}_6$ representa todas las operaciones de rotación *esencialmente distintas*, que son únicamente 6. Si el lector lo medita un poco, este proceso de clasificación de rotaciones equivale a enrollar la recta de los números enteros sobre un hexágono (véase la Figura 3.2).

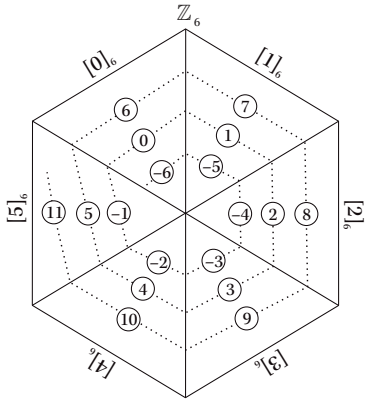


Figura 3.2: Hemos *transformado* el conjunto infinito $\mathbb{Z}$ en el conjunto finito $\mathbb{Z}_6$.

Vamos a proveer al conjunto $\mathbb{Z}_n$ de una estructura algebraica. Más precisamente, vamos a *definir* la suma entre dos elementos P y Q de $\mathbb{Z}_n$. Dados $P = [a]_n$ y $Q = [b]_n$, donde $a, b \in \mathbb{Z}$, definimos $P + Q$ como

$$P + Q = [a]_n + [b]_n := [a + b]_n \in \mathbb{Z}_n.$$

El lector podría cuestionar la seriedad de esta definición con el siguiente razonamiento: para definir $P+Q$ hemos utilizado en esencia los números enteros a y b, donde $[a]_n = P$ y $[b]_n = Q$. Supongamos que $a' \equiv_n a$ y $b' \equiv_n b$.

[13] Note que $\mathbb{Z}_n$ no es un conjunto de números enteros sino un conjunto de clases de congruencia, de modo que cuando nos referimos a un *entero módulo n* en realidad nos referimos a la clase de congruencia módulo n de un número entero.

Entonces $P = [a']_n$, y $Q = [b']_n$, luego *también* sería posible definir la suma $P + Q$ como

$$P + Q = [a']_n + [b']_n := [a' + b']_n \in \mathbb{Z}_n.$$

¿Qué tal que las clases $[a + b]_n$ y $[a' + b']_n$ sean distintas? Esto haría ambigua la definición que proponemos. Pues bien, resulta que dado que $a \equiv_n a'$ y $b \equiv b'$, gracias al Teorema 3.42 (d) tenemos que $a + a' \equiv_n b + b'$, lo cual implica que $[a + b]_n = [a' + b']_n$; esto garantiza que la definición propuesta carece de ambigüedad o, en otras palabras, que es una buena definición.

Buena definición

Observación 3.50. Si $[a]_n = [a']_n$ y $[b]_n = [b']_n$, entonces se tiene que $[a + b]_n = [a' + b']_n$; por ende, la definición de la suma dada por

$$P + Q = [a]_n + [b]_n := [a + b]_n \in \mathbb{Z}_n$$

es una buena definición.

Ejemplo 3.51. Sea $n = 5$. Para calcular la suma de las clases $P = [2]_5$ y $Q = [9]_5$ podemos proceder de varias formas:

(a) Como $2 \in P$ y $9 \in Q$, entonces $P + Q = [2 + 9] = [11]_5$.
(b) Como $2 \in P$ y $4 \in Q$, entonces $P + Q = [2 + 4] = [6]_5$.
(c) Como $-8 \in P$ y $29 \in Q$, entonces $P + Q = [-8 + 29] = [21]_5$.

Por supuesto, $[11]_5 = [6]_5 = [21]_5$ y todas son iguales a $[1]_5$.

Es fácil ver que la suma en $\mathbb{Z}_n$ que hemos definido es conmutativa y asociativa. Por ejemplo, para verificar que ésta es conmutativa, sean $P = [a]_n \in \mathbb{Z}_n$ y $Q = [b]_n \in \mathbb{Z}$. Entonces,

$$\begin{aligned} P + Q &= [a]_n + [b]_n \\ &= [a + b]_n && \text{(Df. suma en } \mathbb{Z}_n) \\ &= [b + a]_n && \text{(Conm.)} \\ &= [b]_n + [a]_n && \text{(Df. suma en } \mathbb{Z}_n) \\ &= Q + P. \end{aligned}$$

Veamos ahora que la suma en $\mathbb{Z}_n$ tiene un elemento identidad:

Teorema 3.52. Si $Q = [0]_n$, entonces para todo $P \in \mathbb{Z}_n$, $P + Q = P$. En otras palabras, el elemento $Q = [0]_n \in \mathbb{Z}_n$ es una identidad de la suma.

Prueba. Basta notar que si $P = [a]_n \in \mathbb{Z}_n$, entonces

$$P + Q = [a]_n + [0]_n = [a + 0]_n = [a]_n = P.$$

■

> ☞ **Antes de seguir leyendo**
>
> Intentemos definir la relación $\leq$ sobre $\mathbb{Z}_n$ de la siguiente manera: dado $P = [a]_n$ y $Q = [b]_n$, diremos que $P \leq Q$ si y sólo si $a \leq b$, según el orden usual de los números enteros. ¿Qué problemas presenta la definición anterior?

Sistema completo de residuos

Definición 3.53. Dado un número natural positivo n, diremos que un conjunto de números enteros R es un *sistema completo de residuos módulo* n si se cumple que

(a) R tiene n elementos;

(b) los elementos de R no son congruentes módulo n entre sí (dicho de otro modo, dados $x, y \in R$, si $x \neq y$, entonces $x \not\equiv_n y$).

Teorema 3.54. Sea $n \in \mathbb{N}^*$ y sea $R = \{a_1, \ldots, a_n\}$ un sistema completo de residuos módulo n. Entonces $\mathbb{Z}_n = \{[a_1]_n, \ldots, [a_n]_n\}$. En particular, para todo $r \in \mathbb{Z}$ con $0 \leq r < n$ existe un único i tal que $[a_i]_n = [r]_n$.

Prueba. Se deja al lector (ejercicio 9). ■

> **Ejemplo 3.55**. El conjunto $R = \{8, 1, -2, 15\}$ es un sistema completo de residuos módulo 4 pues $|R| = 4$ y ninguno de sus elementos es congruente módulo 4 a otro. Además, note que el conjunto $\mathbb{Z}_4$ es $\{[8]_4, [1]_4, [-2]_4, [15]_4\}$ ya que $[8]_4 = [0]_4$, $[1]_4 = [1]_4$, $[-2]_4 = [2]_4$ y $[15]_4 = [3]_4$. Entonces
>
> $$\mathbb{Z}_4 = \{[x]_4 : x \in R\}.$$

El Pequeño Teorema de Fermat

Dado $n \in \mathbb{N}^*$, consideremos el conjunto de todos los números enteros positivos menores o iguales que n, que sean primos relativos con n:

$$R_n := \{a \in \mathbb{Z} : 1 \leq a \leq n, (n, a) = 1\}.$$

A este conjunto lo llamaremos el *sistema canónico reducido de residuos módulo n*. El tamaño de este conjunto puede variar ampliamente, según la naturaleza de n. Por ejemplo, para $n = 16$ tenemos que

R_n: Sistema canónico reducido de residuos

$$R_{16} = \{1, 3, 5, 7, 9, 11, 13, 15\},$$

que es un conjunto con 8 elementos, mientras que si $n = 17$, entonces

$$R_{17} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\},$$

el cual es un conjunto con 16 elementos.

Definición 3.56 (Función φ de Euler). Dado un número natural positivo n, definimos $\varphi(n)$ como la cantidad de números enteros a tales que $1 \leq a \leq n$ y $(a, n) = 1$, es decir, el tamaño del conjunto R_n.

Función φ de Euler

Según esto, por ejemplo, $\varphi(1) = 1$, $\varphi(16) = 8$ y $\varphi(17) = 16$. En general, si n es un número primo, el conjunto R_n tendrá $n - 1$ elementos, luego $\varphi(n) = n - 1$. De modo que podemos pensar informalmente en $\varphi(n)$ como un indicador del *grado de primalidad de n*, según cuánto se aproxime este número a $n - 1$. Es fácil observar que $\varphi(n) = n - 1$ si y sólo si n es un número primo.

Definición 3.57. Dado $n \in \mathbb{N}^*$, diremos que un conjunto de números enteros R es un *sistema reducido de residuos módulo n* si se cumple que:

Sistema reducido de residuos

(a) R tiene $\varphi(n)$ elementos;

(b) para todo $a \in R$, $(a, n) = 1$;

(c) los elementos de R son no congruentes módulo n entre sí (es decir, si $a, b \in R$ y $a \neq b$, entonces $a \not\equiv_n b$).

Teorema 3.58. Sea $k = \varphi(n)$ y sea $R = \{r_1, r_2, \ldots, r_k\}$ un sistema reducido de residuos módulo n. Si a es un número entero tal que $(a, n) = 1$, entonces el conjunto $aR := \{ar_1, ar_2, \ldots, ar_k\}$ es también un sistema reducido de residuos módulo n.

Prueba. Se deja al lector (ejercicio 10). ∎

Veamos que el conjunto R_n es un conjunto reducido de residuos módulo n, esto es, que cumple con las tres propiedades de la definición. Las primeras dos son evidentes. Para la última basta notar que dos números enteros distintos x, y tales que $1 \leq x \leq n$ y $1 \leq y \leq n$ nunca pueden ser congruentes módulo n, ya que su diferencia no puede ser un múltiplo de n.

Ejemplo 3.59. Como ya se mencionó, $R_{16} = \{1,3,5,7,9,11,13,15\}$ y $\varphi(16) = 8$. Sea

$$R = \{-15, 35, 21, 55, 9, -5, 45, 31\}.$$

El conjunto R es un sistema reducido de residuos módulo 16 pues, en primer lugar, $|R| = 8 = \varphi(16)$; en segundo lugar, todos los elementos de R son primos relativos con 13; y, en tercer lugar, no hay ningún par de elementos distintos de R que sean congruentes módulo 16 entre sí. Note además que

$$\text{RES}_{16}(-15) = 1,\ \text{RES}_{16}(35) = 3,\ \text{RES}_{16}(21) = 5,\ \text{RES}_{16}(55) = 7,$$
$$\text{RES}_{16}(9) = 9,\ \text{RES}_{16}(-5) = 11,\ \text{RES}_{16}(13) = 13,\ \text{RES}_{16}(31) = 15.$$

Por ello, el conjunto de los residuos módulo 16 de los elementos de R es precisamente R_{16}, como lo establece de manera general el teorema que sigue.

Teorema 3.60. Dados $n > 1$ y $k = \varphi(n)$, sea $R = \{x_1, x_2, \ldots, x_k\}$ un conjunto reducido de residuos módulo n. Para todo i sea $r_i = \text{RES}_n(x_i)$. Entonces R_n, el conjunto canónico reducido de residuos de n, es precisamente $\{r_1, \ldots, r_k\}$.

Prueba. Sea $R = \{r_1, r_2, \ldots, r_k\}$. Hacemos varias observaciones:

(a) Para todo s, $(r_s, n) = 1$: dado que $(x_s, n) = 1$, por el Teorema 3.18 concluimos que existen $a, b \in \mathbb{Z}$ tales que $ax_s + bn = 1$. Ahora, sea q un número entero tal que $x_s = qn + r_s$. Entonces $a(qn + r_s) + bn = 1$ o, equivalentemente, $(aq + b)n + ar_s = 1$. Gracias nuevamente a dicho teorema, concluimos que $(r_s, n) = 1$.

(b) Para todo s, $1 \leq r_s < n$: esto se tiene ya que r_s es un residuo módulo n y r_s no es 0, puesto que $(x_s, n) = 1$ y por tanto $n \nmid x_s$.

(c) R tiene k elementos: para ello debemos ver que si $s \neq t$, entonces $r_s \neq r_t$. Si $s \neq t$, entonces $x_s \neq x_t$, por ende, $x_s \not\equiv_n x_t$, lo que implica, por una consecuencia de la definición de la relación de congruencia, que $r_s \neq r_t$.

Las observaciones (a) y (b) implican que $R \subseteq R_n$. La observación (c) garantiza que R y R_n tienen el mismo número de elementos. Como ellos son dos conjuntos finitos y uno de ellos está contenido en el otro, entonces deben ser iguales. ∎

Teorema 3.61 (Pequeño Teorema de Fermat, PTF). Si p es un número primo y a es un número natural positivo tal que $(a,p) = 1$, entonces $a^{p-1} \equiv_p 1$.

PTF: *Pequeño Teorema de Fermat*

Prueba. Sabemos que $R_p = \{1, 2, \ldots, p-1\}$. Por el Teorema 3.58, se tiene que el conjunto

$$\{a, 2a, \ldots, (p-1)a\}$$

es un sistema reducido de residuos módulo p. Asimismo, para todo i tal que $1 \leq i \leq p-1$, sea $r_i = \text{RES}_p(ia)$. Es fácil ver que $r_i \equiv_p ia$; luego, gracias a una aplicación repetida del Teorema 3.42 (e) podemos concluir que

$$(a)(2a)\cdots((p-1)a) \equiv_p r_1 r_2 \cdots r_{p-1},$$

o, equivalentemente,

$$a^{p-1}(p-1)! \equiv_p r_1 r_2 \cdots r_{p-1}.$$

Dado que los residuos r_i son todos distintos entre sí y se encuentran entre 1 y $p-1$, podemos afirmar que

$$R_p = \{1, 2, \ldots, p-1\} = \{r_1, r_2, \ldots, r_{p-1}\}.$$

Por ende, $(p-1)! = r_1 r_2 \cdots r_{p-1}$. Entonces

$$a^{p-1}(p-1)! \equiv_p (p-1)!.$$

Dado que $((p-1)!, p) = 1$ (véase el ejercicio 10 de la § 3.3), el Teorema 3.44 permite concluir que

$$a^{p-1} \equiv_p 1.$$ ∎

Veamos ahora una aplicación del PTF:

Ejemplo 3.62. Calcule el residuo $\text{RES}_{13}(6^{542})$, esto es, el mínimo número natural m tal que $6^{542} \equiv_{13} m$.

Solución. Como 13 es un número primo, por el PTF, $6^{12} \equiv_{13} 1$. Ahora, $542 = (45)12 + 2$, luego $6^{542} = (6^{12})^{45} 6^2$. A partir de las congruencias

$$6^{12} \equiv_{13} 1 \quad \text{y} \quad 6^2 \equiv_{13} 6^2,$$

y por el Teorema 3.42 (partes (e) y (f)), concluimos que

$$(6^{12})^{45} 6^2 \equiv_{13} 1^{45} 6^2.$$

Así, $6^{542} \equiv_{13} 36$. Dado que $\text{RES}_{13}(36) = 10$, se tiene que $m = 10$.

Sea $n = 3576$. El último dígito de este número entero es 6. Otra forma de pensar en este número es como el residuo que resulta al dividir a n por 10, esto es, $\text{RES}_{10}(n) = 6$. Como veremos en el siguiente ejemplo, el

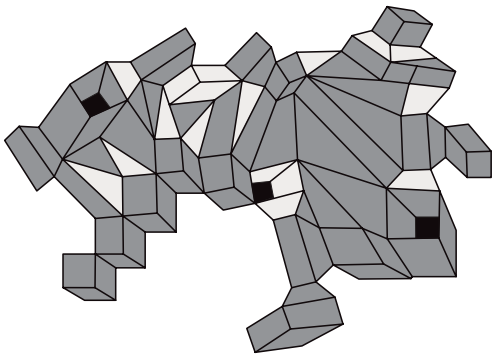
PTF puede utilizarse como un instrumento para calcular el último dígito de algunos números enteros.

Ejemplo 3.63. Determine el último dígito de 3^{21} (es decir, el entero $\text{RES}_{10}(3^{21})$). Lo primero que haremos es calcular $\text{RES}_5(3^{21})$. Por el PTF, $3^4 \equiv_5 1$. Como $3^{21} = (3^4)^5 3$, concluimos que

$$(3^4)^5 3 \equiv_5 1^5 3,$$

luego $3^{21} \equiv_5 3$. Esto significa que 3^{21} es de la forma $5k + 3$, para algún $k \in \mathbb{Z}$; dado que los múltiplos enteros de 5 tienen a 0 o a 5 como último dígito, entonces 3^{21} tiene un 3 o un 8 como último dígito. Pero 3^{21} es un número entero impar (véase el ejercicio 2 de la § 3.1, arriba), luego necesariamente debe tener a 3 como último dígito.

Ejercicios



1. Demuestre que para todo $n \in \mathbb{N}$ se tiene que $11^n \equiv_{100} 10n + 1$.
2. En los siguientes ejercicios, encuentre el residuo que resulta de dividir a n por m:
   (a) $n = 42^{33}$, $m = 3$; (c) $n = 53^{101}$, $m = 24$;
   (b) $n = 26^{17}$, $m = 7$; (d) $n = 76^{82}$, $m = 12$.
3. Utilice el PTF para calcular el último dígito de cada uno de los siguientes números enteros:
   (a) 2^{76}, (c) 7^{138}, (e) 15^{66},
   (b) 43^{15}, (d) 4^{77}, (f) 29^{4501}.

4. Demuestre que, dados $a, b, n \in \mathbb{N}^*$, si $a \equiv_n b$ entonces $(a, n) = (b, n)$. ¿Vale en general el recíproco?
5. Demuestre que para todo $k \in \mathbb{N}^*$, el último dígito de 4^k es 4 o 6.
6. Sea $n \in \mathbb{N}^*$. Demuestre las siguientes afirmaciones:
   (a) n es múltiplo de 3 si y sólo si la suma de los dígitos de n es múltiplo de 3. (*Ayuda*: sea $n = n_0 + 10n_1 + \cdots + 10^k n_k$. Considere el polinomio dado por $p(x) = n_0 + xn_1 + \cdots + x^k n_k$ y utilice el Corolario 3.43.)
   (b) n es múltiplo de 4 si y sólo si $\text{RES}_{100}(n)$ es múltiplo de 4.
7. Sean $n, m \in \mathbb{N}^*$, $a \in \mathbb{Z}$. Demuestre que $m \mid n$, si se tiene que
$$\forall x \in \mathbb{Z} : x \equiv_n a \to x \equiv_m a.$$
8. Demuestre el Teorema 3.45.
9. Demuestre el Teorema 3.54.
10. Demuestre el Teorema 3.58.
11. Sea $n = 10$ y sea $R = \{31, 23, 7, 49\}$.
    (a) Verifique directamente (a partir de la definición) que R es un sistema reducido de residuos módulo n.
    (b) Verifique directamente (a partir de la definición) que $9R$ es un sistema reducido de residuos módulo n (este hecho lo garantiza el Teorema 3.58). (Recuerde que $9R := \{9x : x \in R\}$.)
12. Sean $n \in \mathbb{N}^*$, $k \in \mathbb{Z}$ y $R \subseteq \mathbb{Z}$. Sea $R' = R + kn := \{r + kn : r \in R\}$. Demuestre las siguientes afirmaciones:
    (a) R es un sistema de residuos módulo n si y sólo si R' es un sistema de residuos módulo n.
    (b) R es un sistema reducido de residuos módulo n si y sólo si R' es un sistema reducido de residuos módulo n.

§ 3.6 El Teorema Chino del Residuo

Definición 3.64. Sea n un número natural positivo y sean $a, b \in \mathbb{Z}$. Diremos que *la congruencia lineal* $ax \equiv_n b$ *tiene una solución* si existe $e \in \mathbb{Z}$ tal que $ae \equiv_n b$.

Supongamos que $e \in \mathbb{Z}$ es una solución de la congruencia $ax \equiv_n b$, y sea $e' \in \mathbb{Z}$ tal que $e \equiv_n e'$. Sea $s \in \mathbb{Z}$ tal que $e' - e = sn$. Entonces $e' = e + sn$, luego $ae' = ae + asn$ y por ende, $ae' \equiv_n ae$. Pero entonces $ae' \equiv_n b$. Luego e' es también una solución de la congruencia $ax \equiv_n b$. En resumen:

Observación 3.65. Consideremos la congruencia lineal $ax \equiv_n b$. Si e es una solución de esta congruencia y $e' \in [e]_n$, entonces e' es también una solución.

Esta observación nos permite ahora definir sin ambigüedad el concepto de *clase-solución de una congruencia lineal*:

Definición 3.66. Sea n un número natural positivo y sean $a, b \in \mathbb{Z}$. Consideremos la congruencia lineal $ax \equiv_n b$. Dado $P \in \mathbb{Z}_n$ con $P = [e]_n$, diremos que P es una *clase-solución de la congruencia* $ax \equiv_n b$ si e es una solución de la congruencia $ax \equiv_n b$.

Clase-solución

Definición 3.67. Diremos que la congruencia lineal $ax \equiv_n b$ *tiene exactamente k soluciones módulo n* si existen exactamente k elementos $P \in \mathbb{Z}_n$ tales que P es una clase-solución de $ax \equiv_n b$; en otras palabras, si el conjunto

$$\{P \in \mathbb{Z}_n : P \text{ es una clase-solución de } ax \equiv_n n\}$$

tiene exactamente k elementos.

☞ **Antes de seguir leyendo**

Sea n un número natural positivo, y $a, b \in \mathbb{Z}$. Demuestre las siguientes afirmaciones:

1. Si la congruencia $ax \equiv_n b$ tiene al menos una solución $e \in \mathbb{Z}$, entonces tiene infinitas soluciones.
2. La congruencia $ax \equiv_n b$ tiene finitas clases-soluciones.

Ejemplo 3.68. Considere la congruencia $12x \equiv_8 20$. Estamos interesados en saber cuántas clases-soluciones tiene esta congruencia. Para ello consideramos cada elemento de $\mathbb{Z}_8$ e indagamos si es clase-solución de ella, así:

$[0]_8$: tenemos que $12(0) = 0 \not\equiv_8 20$;
$[1]_8$: tenemos que $12(1) = 12 \equiv_8 20$;
$[2]_8$: tenemos que $12(2) = 24 \not\equiv_8 20$;
$[3]_8$: tenemos que $12(3) = 36 \equiv_8 20$;
$[4]_8$: tenemos que $12(4) = 48 \not\equiv_8 20$;

$[5]_8$: tenemos que $12(5) = 60 \equiv_8 20$;

$[6]_8$: tenemos que $12(6) = 72 \not\equiv_8 20$;

$[7]_8$: tenemos que $12(7) = 84 \equiv_8 20$.

Concluimos que la congruencia $12x \equiv_8 20$ tiene exactamente 4 soluciones módulo 8.

El siguiente teorema establece precisamente cuándo una congruencia lineal tiene por lo menos una solución:

Teorema 3.69. Sea n un número natural positivo y sean $a, b \in \mathbb{Z}$. Consideremos la congruencia lineal $ax \equiv_n b$. Sea $d = (a, n)$. Entonces la congruencia tiene por lo menos una solución si y sólo si $d \mid b$.

Prueba. Utilizamos el método de doble implicación:

($\rightarrow$) Supongamos que existe $e \in \mathbb{Z}$ tal que $ae \equiv_n b$. Sea $c \in \mathbb{Z}$ tal que $b - ae = cn$. Así, $b = cn + ae$ y, como $d = (a, n)$, entonces $d \mid b$, en virtud del Teorema 3.3 (f).

($\leftarrow$) Supongamos que $d \mid b$ y sea $c \in \mathbb{Z}$ tal que $dc = b$. Como $d = (a, n)$, entonces d puede expresarse como una combinación lineal entre a y n, esto es, existen $s, t \in \mathbb{Z}$ tales que $d = sa + tn$. Entonces

$$b - asc = dc - asc = (d - as)c = tnc.$$

Luego $n \mid (b - a(sc))$ y así, por el Teorema 3.41, $a(sc) \equiv_n b$. Por ende, sc es una solución de la congruencia $ax \equiv_n b$. ∎

Si una congruencia lineal tiene por lo menos una solución conocida, a partir de ella podemos describir todas sus soluciones.

Teorema 3.70. Sea n un número natural positivo y sean $a, b \in \mathbb{Z}$. Consideremos la congruencia lineal $ax \equiv_n b$. Sea $d = (a, n)$. Entonces la congruencia tiene por lo menos una solución e si y sólo si $d \mid b$. En este caso, la congruencia tiene exactamente d soluciones módulo n y, además, las d clases-solución de la congruencia son

$$\left[e\right]_n, \left[e + \frac{n}{d}\right]_n, \left[e + \frac{2n}{d}\right]_n, \ldots, \left[e + \frac{(d-1)n}{d}\right]_n,$$

en donde $e \in \mathbb{Z}$ es cualquier solución de la congruencia.

Prueba. El Teorema 3.69 garantiza la primera parte del resultado, esto es, que la congruencia tiene solución si y sólo si $d \mid b$. Para demostrar la otra parte, supongamos que $e \in \mathbb{Z}$ es una solución de la congruencia.

Debemos ver que ésta tiene exactamente d soluciones módulo n y que las d clases-solución de ella son exactamente aquellas de la forma

$$\left[e + \frac{in}{d}\right]_n \quad (0 \leq i < d).$$

Primero debemos observar que hay realmente d clases como las anteriormente descritas y no menos: sean i, i' tales que $0 \leq i < d$ y $0 \leq i < d$, y supongamos que las clases $[e + \frac{in}{d}]_n$ y $[e + \frac{i'n}{d}]_n$ son iguales, es decir, que $e + \frac{in}{d} \equiv_n e + \frac{i'n}{d}$. Entonces $(i' - i)\frac{n}{d} = cn$ para algún $c \in \mathbb{Z}$, luego $|i' - i| = d|c|$. Ahora, es claro que $|i' - i| < d$, lo cual implica que $|i - i'| = 0$, es decir, $i = i'$. El resultado anterior puede reformularse de esta manera:

$$\text{si } 0 \leq i, i' < d \text{ e } i \neq i', \text{ entonces } \left[e + \frac{in}{d}\right]_n \neq \left[e + \frac{i'n}{d}\right]_n,$$

lo cual quiere decir que las clases así descritas son *exactamente* d. Para terminar la demostración basta verificar que, para todo $e' \in \mathbb{Z}$, e' es una solución de la congruencia si y sólo si existe i tal que $0 \leq i < d$ y $e' \equiv_n e + \frac{in}{d}$. Para ello utilizamos el método de doble implicación:

($\rightarrow$) Supongamos que e' es una solución de la congruencia. Entonces $ae' \equiv_n b \equiv_n ae$. De modo que $ae \equiv_n ae'$, luego por el Teorema 3.45, $e \equiv_{\frac{n}{d}} e'$. Entonces existe $c \in \mathbb{Z}$ tal que $e' - e = \frac{cn}{d}$. Ahora, por el Algoritmo de la División, c es de la forma

$$c = hd + i, 0 \leq i < d.$$

Entonces tenemos que $e' - e = (hd + i)\frac{n}{d} = hn + \frac{in}{d}$ o, equivalentemente, $e + \frac{in}{d} - e' = -hn$, lo cual demuestra que $e' \equiv_n e + \frac{in}{d}$.

($\leftarrow$) Supongamos que existe i tal que $0 \leq i < d$ y $e' \equiv_n e + \frac{in}{d}$. Para ver que e' es solución de la congruencia, basta verificar, por la Observación 3.65, que $e + \frac{in}{d}$ lo es. En efecto,

$$a\left(e + \frac{in}{d}\right) = ae + n\left(\frac{ia}{d}\right) \equiv_n b + 0 = b. \qquad \blacksquare$$

En lo que sigue consideramos sistemas de varias congruencias lineales. Veamos algunos ejemplos:

Ejemplo 3.71. Encuentre todas las soluciones del siguiente sistema de congruencias lineales:

$$x \equiv_{12} 1,$$
$$x \equiv_9 4.$$

Solución. Supongamos que existe $a \in \mathbb{Z}$ tal que a es una solución del sistema de congruencias. Entonces existe $b \in \mathbb{Z}$ tal que $a = 12b + 1$. Dado que $a \equiv_9 4$, tenemos que $12b + 1 \equiv_9 4$, luego $12b \equiv_9 3$. Por ende,

$$3b = 12b - 9b \equiv_9 3 - 9b \equiv_9 3 - 0 = 3.$$

Esto implica que existe $k \in \mathbb{Z}$ tal que $3b - 3 = 9k$, de modo que $b - 1$ debe ser un múltiplo de 3. Si tomamos, por ejemplo, $b = 1$, obtenemos $a = 13$, el cual claramente es una solución del sistema de congruencias. Además, hemos demostrado que toda solución debe ser de la forma $12b + 1$, en donde b es múltiplo de 3, digamos $b - 1 = 3c$, $c \in \mathbb{Z}$. Luego

$$a = 12(3c + 1) + 1 = 13 + 36c.$$

Para demostrar que todo número entero de la forma $a = 13 + 36c$ ($c \in \mathbb{Z}$) es una solución del sistema de congruencias, observamos lo siguiente:

$$13 + 36c = 4 + 9(1 + 4c) \equiv_9 4 + 0 = 4;$$
$$13 + 36c = 1 + 12(1 + 3c) \equiv_{12} 1 + 0 = 1.$$

Por ende, el conjunto de soluciones del sistema de congruencias es

$$\{13 + 36c : c \in \mathbb{Z}\}.$$

Ejemplo 3.72. Resuelva este sistema de congruencias lineales:

$$x \equiv_{20} 2,$$
$$x \equiv_{18} 3.$$

Solución. Supongamos que existe $a \in \mathbb{Z}$ tal que a es una solución del sistema de congruencias. Entonces existe $b \in \mathbb{Z}$ tal que

$$a = 20b + 2.$$

Dado que $a \equiv_{18} 3$, tenemos que $20b + 2 \equiv_{18} 3$, luego $20b \equiv_{18} 1$ y, por ende,

$$2b = 20b - 18b \equiv_{18} 1 - 18b \equiv_{18} 1 - 0 = 1.$$

Esto implica que existe $k \in \mathbb{Z}$ tal que $2b = 18k + 1$ lo cual es imposible pues 1 es impar. Concluimos que el sistema anterior es *inconsistente*, es decir, no tiene solución alguna.

En el ejemplo 3.71, los módulos del sistema de congruencias (12 y 9) no son primos relativos entre sí. En el ejemplo 3.72 se presenta la

misma situación. En general, si los módulos involucrados en un sistema de congruencias lineales no son primos relativos entre sí, entonces el sistema puede o no tener solución. Sin embargo, como veremos más adelante, si los módulos involucrados en un sistema de congruencias lineales son primos relativos entre sí, entonces el sistema tiene solución.

Si dos números enteros a y b mantienen entre sí múltiples congruencias respecto de módulos que son primos relativos, entonces a y b son congruentes respecto del producto de los módulos:

Teorema 3.73. Sean $n_1, \ldots, n_k$ números naturales positivos tales que para $s \neq t$ tenemos que $(n_s, n_t) = 1$, y sean $a, b \in \mathbb{Z}$ tales que para todo i, $a \equiv_{n_i} b$. Entonces $a \equiv_n b$, donde $n = n_1 \cdots n_k$.

Prueba. Se demuestra por inducción en k:

(a) Caso base ($k = 1$). Es evidente.

(b) Paso inductivo: supongamos que el resultado es verdadero para $k \in \mathbb{N}^*$ y demostrémoslo para $k+1$. Supongamos que $n_1, \ldots, n_k, n_{k+1}$ son enteros positivos primos relativos entre sí, y sean $a, b \in \mathbb{Z}$ tales que $a \equiv_{n_i} b$, $1 \leq i \leq k+1$. Sea $n' = n_1 n_2 \cdots n_k$. Por hipótesis de inducción concluimos que $a \equiv_{n'} b$. Sean $e, e' \in \mathbb{Z}$ tales que

$$b - a = e n_{k+1} \text{ y } b - a = e' n'.$$

Entonces $e n_{k+1} = e' n'$, luego $n_{k+1} \mid e' n'$. Y así $(n_{k+1}, n') = 1$; luego, por el Teorema 3.19, $n_{k+1} \mid e'$. A partir de las hipótesis es fácil concluir que existe $c \in \mathbb{Z}$ tal que $c n_{k+1} = e'$. Entonces

$$b - a = e' n' = c n_{k+1} n' = c(n_1 n_2 \cdots n_k n_{k+1}),$$

como queríamos demostrar. ∎

Teorema 3.74. Sean $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ y sean $n_1, n_2, \ldots, n_k \in \mathbb{N}^*$. Consideremos el siguiente sistema de congruencias lineales:

$$\begin{aligned} x &\equiv_{n_1} a_1, \\ x &\equiv_{n_2} a_2, \\ &\cdots \\ x &\equiv_{n_k} a_k. \end{aligned}$$

Sea $n = n_1 n_2 \cdots n_k$ y sea $s \in \mathbb{Z}$ una solución del sistema anterior. Entonces, para todo $x \in \mathbb{Z}$, tal que $x \equiv_n s$, se tiene que x es una solución de la congruencia.

Prueba. Si $x \equiv_n s$, entonces $n \mid s - x$. Para todo i tenemos que $n_i \mid n$; luego $n_i \mid s - x$, lo cual implica que $x \equiv_{n_i} s$. Como s es una solución del sistema de congruencias, entonces x también lo es, como queríamos ver. ∎

El siguiente teorema establece condiciones suficientes para resolver un sistema de varias congruencias lineales. Su nombre procede de que su demostración fue dada por el matemático chino Sun Tzu alrededor del siglo III DC:

TCR: *Teorema Chino del Residuo*

Teorema 3.75 (Teorema Chino del Residuo, TCR). Sean $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, y sean $n_1, n_2, \ldots, n_k \in \mathbb{N}^*$ tales que para todo $s \neq t$, $(n_s, n_t) = 1$. Consideremos el siguiente sistema de congruencias lineales:

$$\begin{aligned} x &\equiv_{n_1} a_1, \\ x &\equiv_{n_2} a_2, \\ &\cdots \\ x &\equiv_{n_k} a_k. \end{aligned}$$

Entonces el sistema tiene una solución. Además, el conjunto de todas las soluciones del sistema de congruencias es precisamente $[s]_n$, donde $s \in \mathbb{Z}$ es cualquier solución del sistema y $n = n_1 n_2 \cdots n_k$.

Prueba. Sea $n = n_1 n_2 \cdots n_k$. Fijamos un $i \in \mathbb{N}$, tal que $1 \leq i \leq k$, y hacemos el siguiente análisis. Sea

$$s_i = n/n_i = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k.$$

Es fácil ver que $(n_i, s_i) = 1$. Sea $R_{n_i} = \{r_1, \ldots, r_z\}$ el sistema canónico reducido de residuos módulo n_i. Por el Teorema 3.58, el conjunto

$$s_i R_{n_i} = \{s_i r_1, \ldots, s_i r_z\}$$

es también un sistema reducido de residuos módulo n_i. Ahora, como $1 \in R_{n_i}$, entonces por el Teorema 3.60 existe $b \in s_i R_{n_i}$ tal que $1 = \text{RES}_{n_i}(b)$. Este elemento b será por supuesto de la forma $s_i r_t$ y $s_i r_t \equiv_{n_i} 1$. En resumen, para todo i hemos encontrado un número entero c_i tal que $s_i c_i \equiv_{n_i} 1$. Por ende, para todo i tenemos que $s_i c_i a_i \equiv_{n_i} a_i$. Ahora, sea

$$s = \sum_{i=1}^{k} s_i c_i a_i.$$

Para todo i, tenemos que $s_i c_i a_i \equiv_{n_i} a_i$ y, si $j \neq i$, entonces $s_j c_j a_j \equiv_{n_i} 0$. Luego, por el Teorema 3.42 (d) aplicado repetidas veces, concluimos que $s \equiv_{n_i} a_i$. Esto demuestra que s es una solución del sistema.

Sea $s \in \mathbb{Z}$ cualquier solución del sistema, y sea $\text{SOL} \subseteq \mathbb{Z}$ el conjunto de todas las soluciones al sistema. Gracias al Teorema 3.73, $\text{SOL} \subseteq [s]_n$; el Teorema 3.74 garantiza que $[s]_n \subseteq \text{SOL}$. Concluimos que $\text{SOL} = [s]_n$. ∎

En particular, si consideramos un sistema de congruencias como el del enunciado del TCR, entonces la solución de éste es única módulo $n = n_1 \cdots n_k$. Esto se debe a que si $s, s' \in \text{SOL}$, entonces $\text{SOL} = [s]_n$; luego $s' \in [s]_n$, es decir, $s \equiv_n s'$.

Veamos ahora un ejemplo de cómo encontrar las soluciones de un sistema de congruencias lineales:

Ejemplo 3.76. Encuentre todas las soluciones del siguiente sistema de congruencias lineales:

$$x \equiv_3 2,$$
$$x \equiv_4 3,$$
$$x \equiv_7 2.$$

Solución. Dado que 3, 4 y 7 son primos relativos entre sí, por el TCR sabemos que el sistema tiene una solución $s \in \mathbb{Z}$. Razonamos de la siguiente manera para encontrarla:

(1) Como $s \equiv_3 2$, existe $a \in \mathbb{Z}$ tal que $s = 3a + 2$.

(2) Por (1) tenemos que $3a + 2 \equiv_4 3$. Manipulamos esta congruencia de la siguiente forma para despejar a:

$$\begin{aligned}
3a + 2 \equiv_4 3 &\to 3a + 2 - 2 \equiv_4 3 - 2 && \text{(Sumar } -2\text{, Teo. 3.42 (d))}\\
&\to 3a \equiv_4 1\\
&\to -a \equiv_4 1 - 4a && \text{(Sumar } -4a\text{, Teo. 3.42 (d))}\\
&\to -a \equiv_4 1 + 0 && (-4a \equiv_4 0\text{, Teo. 3.42 (d))}\\
&\to -a \equiv_4 1\\
&\to a \equiv_4 -1 && \text{(Mult. por } -1\text{, Teo. 3.42 (e))}\\
&\to a + 4 \equiv_4 3 && \text{(Sumar 4, Teo. 3.42 (d))}\\
&\to a \equiv_4 3. && (4 \equiv_4 0\text{, Teo. 3.42 (d))}
\end{aligned}$$

(3) Por (2) existe $b \in \mathbb{Z}$ tal que $a = 4b + 3$, luego

$$s = 3(4b + 3) + 2 = 12b + 11.$$

(4) Entonces $12b + 11 \equiv_7 2$. Ahora despejamos b:

$$\begin{aligned}
12b + 11 \equiv_7 2 &\to 12b + 14 \equiv_7 5 && \text{(Sumar 3, Teo. 3.42 (d))}\\
&\to 12b \equiv_7 5 && (14 \equiv_7 0\text{, Teo. 3.42 (d))}\\
&\to 5b \equiv_7 5 - 7b && \text{(Sumar } -7b\text{, Teo. 3.42 (d))}\\
&\to 5b \equiv_7 5 && (-7b \equiv_7 0\text{, Teo. 3.42 (d))}\\
&\to b \equiv_7 1. && \text{(Teo. 3.44, } (5,7) = 1)
\end{aligned}$$

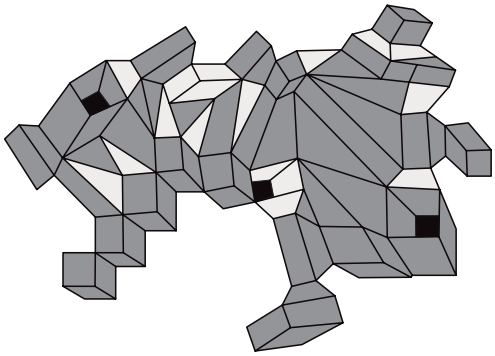
(5) Por (4) existe $c \in \mathbb{Z}$ tal que $b = 7c + 1$. De esta manera tenemos que $s = 12(7c + 1) + 11 = 84c + 23$. En este caso $n = (3)(4)(7) = 84$ y, por lo tanto, $23 \equiv_n s$. Concluimos, de nuevo por el TCR que

23 es una solución del sistema de congruencias; de hecho, el conjunto de todas las soluciones del sistema de congruencias es

$$[23]_{84} = \{23 + 84z : z \in \mathbb{Z}\}.$$

De aquí se sigue que 23 es la única solución x del sistema, tal que $0 \leq x < 84$.

Ejercicios



1. Encuentre las soluciones módulo 24 de la congruencia $42x \equiv_{24} 18$.
2. Sean $a \in \mathbb{Z}$ y $n \in \mathbb{N}^*$. Demuestre que $(a, n) = 1$ si y sólo si para todo $b \in \mathbb{Z}$ la congruencia $ax \equiv_n b$ tiene solución.
3. Sean $n, m \in \mathbb{N}^*$, $a \in \mathbb{Z}$ y supongamos que $n \mid m$. Sean asimismo $X = \{x \in \mathbb{Z} : x \not\equiv_n a\}$ y $Y = \{x \in \mathbb{Z} : x \not\equiv_m a\}$. Demuestre que $X \subseteq Y$. Si $X = Y$, ¿se sigue necesariamente que $n = m$?
4. Encuentre todas las soluciones de los siguientes sistemas de congruencias lineales:
   (a) $x \equiv_5 2$, $x \equiv_6 4$, $x \equiv_7 3$;
   (b) $x \equiv_{10} 6$, $x \equiv_3 1$, $x \equiv_{11} 0$;
   (c) $x \equiv_8 7$, $x + 1 \equiv_5 4$, $x + 3 \equiv_{21} 10$;
   (d) $x \equiv_{10} 2$, $x \equiv_{15} 12$.

   (Note que, si bien en este último caso no se satisfacen las condiciones del TCR, esto no implica que el sistema no tenga solución.)

5. Encuentre todas las soluciones del siguiente sistema de congruencias lineales:

$$x \equiv_6 8,$$
$$x \equiv_5 1,$$
$$x \equiv_{13} 7,$$
$$x \equiv_{11} 4.$$

6. Entre 8000 y 9000 naves espaciales alienígenas se encuentran actualmente en la Tierra. A un mago llamado Kandú, que nunca se equivoca, le preguntaron cuántas eran, y dijo: "Por respeto a la comunidad alienígena, todo lo que puedo decir es que el número de ellas termina en 2". Además, se sabe que las naves se han agrupado hasta ahora en trece frentes de igual número, junto con una nave adicional que hasta ahora ha permanecido sola y ha sido bautizada como Nebbia. Finalmente el DAS ha descifrado, luego de un arduo trabajo, un mensaje alienígena que dice lo siguiente: "estamos esperando a 100 naves más para así visitar las 7 maravillas del mundo en 7 grupos parejos (cada uno con exactamente el mismo número de naves)". ¿Puede usted determinar el número exacto de naves que se encuentran en la Tierra?
7. En un pueblo se realiza un festival gastronómico cada 12 años, y un festival musical cada 20 años. Si en 1820 se realizó por primera vez el festival gastronómico, y en 1826 se realizó por primera vez el festival musical, demuestre que es imposible que en un mismo año se realicen ambos festivales.
8. En un salón hay cierta cantidad de personas, todas ellas sentadas. Supongamos que para todo $n \in \{1, 2, 3, 4, 5\}$ sucede lo siguiente: si las personas se comienzan a retirar de la sala en grupos de $n+1$ personas, en algún momento quedarán exactamente n personas en el salón. Sin embargo, si las personas se comienzan a retirar de la sala en grupos de 7 personas, en algún momento no quedarán personas en la sala. ¿Cuál es el mínimo número posible de sillas que hay en la sala?
9. El gigante David canta cada cinco días y baila cada ocho. Si el día de hoy David cantó, y dentro de dos días bailará, ¿cuál es el mínimo número de días que debemos esperar para que David cante y baile en un mismo día?
10. Ana canta cada seis días, toca piano cada quince y baila cada ocho. Si el día de hoy Ana cantó, hace dos días tocó piano y dentro de cuatro bailará, ¿cuál es el mínimo número de días que debemos esperar para que Ana cante, toque piano y baile en un mismo día?

Para los siguientes ejercicios se requiere que el lector conozca las nociones de función inyectiva, sobreyectiva y biyectiva. Para ello, consulte la § 4.43, abajo.

11. Sean $n, m \in \mathbb{N}^*$, y sea $\text{NAT} : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m$ la función dada por

$$\text{NAT}(x) = ([x]_n, [x]_m) \ (x \in \mathbb{Z}).$$

Sea además $c = \text{MCM}(n, m)$.

   (a) Demuestre que NAT no es una función inyectiva.

   (b) Sea $\text{NAT}_c : \mathbb{Z}_c \to \mathbb{Z}_n \times \mathbb{Z}_m$ la función definida como $\text{NAT}_c([x]_c) = \text{NAT}(x)$. Demuestre que la anterior definición no es ambigua, esto es, que si se tiene $[x]_c = [y]_c$, entonces $\text{NAT}(x) = \text{NAT}(y)$.

   (c) Demuestre que la función $\text{NAT}_c : \mathbb{Z}_c \to \mathbb{Z}_n \times \mathbb{Z}_m$ es inyectiva.

   (d) Concluya a partir del ejercicio anterior una versión particular del TCR, cuando $k = 2$, es decir, cuando el sistema tiene únicamente dos congruencias. (*Ayuda*: utilice el subejercicio anterior y un argumento de conteo para demostrar que bajo las hipótesis del TCR la función NAT_c es biyectiva. De hecho, se puede generalizar este ejercicio si consideramos una función $\text{NAT}_n : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, donde n es el mínimo común múltiplo generalizado entre $n_1, \ldots, n_k$, y esto permite concluir el TCR para cualquier $k \in \mathbb{N}^*$.)

12. **Teorema Resumen, primos relativos.** Sean $n, m \in \mathbb{N}^*$, y sean NAT y NAT_c las funciones definidas en el ejercicio anterior. Demuestre que las siguientes afirmaciones son equivalentes entre sí:

   (a) $(n, m) = 1$.

   (b) $(n) + (m) = \mathbb{Z}$. (Por definición tenemos que $(n) := \{kn : k \in \mathbb{Z}\}$ y $(n) + (m) := \{x + y : x \in (n), y \in (m)\}$.)

   (c) n y m no tienen divisores primos en común.

   (d) $(n) \cap (m) = (nm)$.

   (e) Todo número entero es una combinación lineal entre n y m.

   (f) $\text{MCM}(n, m) = nm$.

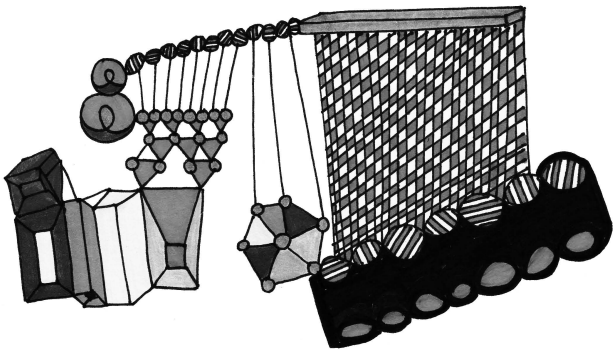
   (g) La función $\text{NAT} : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m$ es sobreyectiva.

   (h) Existe $x \in \mathbb{Z}$ tal que $\text{NAT}(x) = ([1]_n, [0]_m)$ y existe $x \in \mathbb{Z}$ tal que $\text{NAT}(x) = ([0]_n, [1]_m)$.

   (i) Existe $c \in \mathbb{Z}$ tal que $\text{NAT}_c : \mathbb{Z}_c \to \mathbb{Z}_n \times \mathbb{Z}_m$ es sobreyectiva.

   (j) Existe $c \in \mathbb{Z}$ tal que $\text{NAT}_c : \mathbb{Z}_c \to \mathbb{Z}_n \times \mathbb{Z}_m$ es biyectiva.

Proyecto: Clausura e ideales en $\mathbb{Z}$



Este proyecto presenta un enfoque algebraico y también conjuntista al tema de divisibilidad, ya que los resultados son establecidos en términos de ciertos conjuntos canónicos de números enteros (clausura, ideales e ideales primos) cuyos elementos comparten cierta propiedad definida a partir de las operaciones básicas en $\mathbb{Z}$ (suma y multiplicación). En este sentido, nuestros objetos de estudio, en vez de ser los números enteros, serán las clausuras y los ideales.

Definiciones para referencia

Sean $A \subseteq \mathbb{Z}$, $a \in \mathbb{Z}$. Definimos los siguientes conjuntos y propiedades:

(i) La *clausura* de A: $\text{CL}(A) = \{x_1 a_1 + \cdots + x_n a_n : x_i \in \mathbb{Z}, a_i \in A, 1 \leq i \leq n\}$. (Si $A = \varnothing$, definimos $\text{CL}(A) := \{0\}$.)[14]

(ii) A es *cerrado* si $\text{CL}(A) = A$.

(iii) A es un *ideal* si $A \neq \varnothing$ y además, dados $x, a, a' \in \mathbb{Z}$, se tiene que

$$(a \in A \wedge a' \in A) \to (a + a' \in A \wedge ax \in A).$$

(iv) A es un *ideal propio* si A es un ideal tal que $A \neq \mathbb{Z}$.

(v) A es un *ideal primo* si A es un ideal tal que $A \neq \mathbb{Z}$ y dados $x, y \in \mathbb{Z}$ se tiene que, si $x \notin A$ y $y \notin A$, entonces $xy \notin A$.

(vi) A es un *ideal maximal* si A es un ideal tal que $A \neq \mathbb{Z}$, y para todo ideal B tal que $A \subseteq B$ se tiene que $A = B$ o $B = \mathbb{Z}$.

(vii) $(a) = a\mathbb{Z} = \{ka : k \in \mathbb{Z}\}$. Se demuestra que (a) es un ideal, llamado el *ideal principal generado por a*.

(viii) A es un *ideal no trivial* si A es un ideal tal que $A \neq (0)$ y $A \neq (1)$.

[14] Recomendamos enfáticamente al lector hacer el ejercicio 11 de la § 3.2 para familiarizarse con la noción de clausura.

Problemas

1. Demuestre que dados $A, B \subseteq \mathbb{Z}$ las siguientes afirmaciones son equivalentes:
   (a) $\text{CL}(A) = \text{CL}(B)$.
   (b) Todo elemento de A puede escribirse como combinación lineal entre elementos de B, y todo elemento de B puede escribirse como combinación lineal entre elementos de A.
2. Demuestre mediante un contraejemplo que la siguiente afirmación no es válida en general: "Sea $A = \{a_1, \ldots, a_n\} \subseteq \mathbb{Z}$, con $n \in \mathbb{N}^*$. Si para todo $i, j \in \{1, \ldots, n\}$ se tiene que $\text{CL}(\{a_i, a_j\}) \neq \mathbb{Z}$, entonces $\text{CL}(A) \neq \mathbb{Z}$."
3. Dado $A \subseteq \mathbb{Z}$, diremos que A es un *ideal* si $A \neq \varnothing$, dados $a \in A$ y $z \in \mathbb{Z}$, entonces $az \in A$, y dados $a, a' \in A$, entonces $a + a' \in A$.
   (a) Sea $a \in \mathbb{Z}$. Demuestre que el conjunto $(a) = a\mathbb{Z} = \{ak : k \in \mathbb{Z}\}$ es un ideal. (Éste es llamado el *ideal principal generado por a*.)
   (b) Demuestre que para todo ideal $A \subseteq \mathbb{Z}$ existe $a \in \mathbb{Z}$ tal que $A = (a)$.
4. Sean $a, b \in \mathbb{Z}$.
   (a) Calcule (0) y (1), los llamados ideales triviales.
   (b) Demuestre que $(0) \subset (12) \subset (6) \subset (3) \subset (1)$. (Recuerde que $\subset$ denota inclusión estricta).
   (c) Sea $b \neq 0$. Demuestre que $(a) \subseteq (b)$ si y sólo si $b \mid a$.
   (d) Demuestre que $(a) \cap (b)$ es un ideal. Encuentre $c \in \mathbb{Z}$ en términos de a y b tal que $(a) \cap (b) = (c)$.
5. Dado un ideal $A = (a) \subseteq \mathbb{Z}$ (con $a \in \mathbb{Z}$), diremos que A es un *ideal primo* si $A \neq \mathbb{Z}$ y, además, se tiene que para todo $x, y \in \mathbb{Z}$, si $xy \in A$ entonces $(x \in A \vee y \in A)$.[15] Demuestre que (a) es un ideal primo si y sólo si $a = 0 \vee |a|$ es un número primo.
6. Demuestre que si $(a) \subseteq \mathbb{Z}$ es un ideal propio (es decir, $1 \notin (a)$), entonces existe un ideal primo $(b) \subseteq \mathbb{Z}$ tal que $(a) \subseteq (b)$. (En otras palabras, todo ideal propio está contenido en algún ideal primo). (*Ayuda*: utilice el TFA.)
7. Demuestre que todo ideal primo $(a) \subseteq \mathbb{Z}$ tal que $a \neq 0$ cumple la siguiente propiedad: si (b) es un ideal tal que $(a) \subseteq (b)$, entonces $(a) = (b)$ o $(b) = (1) = \mathbb{Z}$.

[15] Esta definición es equivalente a la dada anteriormente.

8. Diremos que $A \subseteq \mathbb{Z}$ es *cerrado* si $\text{CL}(A) = A$. Sea $\mathcal{C}$ el conjunto de todos los subconjuntos cerrados de $\mathbb{Z}$. Demuestre que

$$\mathcal{C} = \{\text{CL}(X) : X \in \mathcal{P}(\mathbb{Z})\} = \{I \in \mathcal{P}(\mathbb{Z}) : I \text{ es un ideal}\}.$$

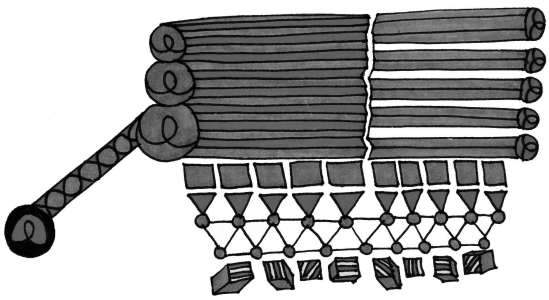
(Esto demuestra que las afirmaciones "A es cerrado", "A es la clausura de un subconjunto de $\mathbb{Z}$", "A es un ideal" y "existe $a \in \mathbb{Z}$ tal que A es el conjunto de todos los elementos de la forma ka ($k \in \mathbb{Z}$)" son equivalentes entre sí.)

9. Sea $\mathcal{D}$ el conjunto de todos los ideales $I \subseteq \mathbb{Z}$ tales que $I \neq (0)$; sea $\mathcal{P}r$ el conjunto de todos los ideales $I \subseteq \mathbb{Z}$ tales que I es un ideal primo e $I \neq (0)$ (note que $\mathcal{P}r \subseteq \mathcal{D}$), y sea $P \subseteq \mathbb{Z}$ el conjunto de todos los números primos. Demuestre que las estructuras ordenadas $(\mathcal{D}, \supseteq)$ y $(\mathbb{N}^*, |)$ son isomorfas. Para ello, defina un isomorfismo

$$\varphi : \mathbb{N}^* \to \mathcal{D},$$

tal que $\varphi[P] = \mathcal{P}r$ (donde por definición $\varphi[P] := \{\varphi(p) : p \in P\}$). (Debe demostrar que la función φ es un isomorfismo entre estructuras ordenadas).

Lecturas adicionales

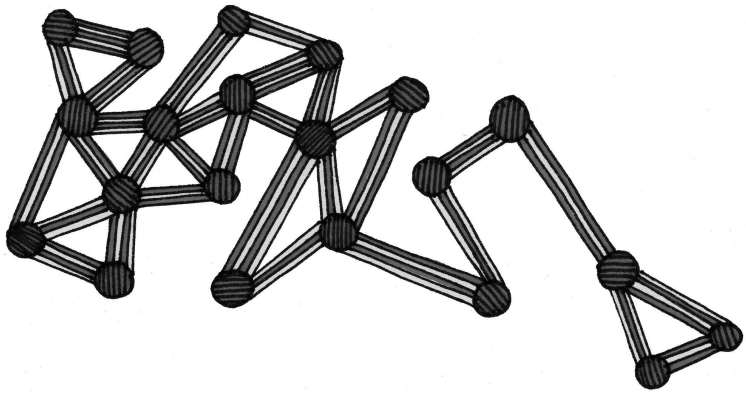


Se recomienda consultar las siguientes lecturas, con miras a profundizar en algunos de los temas tratados en este capítulo:

- Para más información sobre divisibilidad, consulte [5], c. 2; [8], §§ 2.6–2.9; [11], §§ 31–32.
- Para más información sobre congruencias, la Función de Euler y TCR, consulte [5], c. 3 y 4; [8], §§ 2.10–2.15; [11], §§ 33–34.

CAPÍTULO 4

RELACIONES Y FUNCIONES



Conexiones entre conjuntos...

El concepto de relación surge de manera natural en el análisis de ciertas estructuras. Por ejemplo, en el conjunto $\mathbb{N}$ de los números naturales, podemos pensar en la relación *ser menor o igual a*. Bajo esta relación, por ejemplo, 2 se relaciona con 3 pero no al contrario y 0 se relaciona con todos los elementos de $\mathbb{N}$. En el conjunto de los seres humanos, por ejemplo, la relación *tener el mismo padre* permite pensar en los seres humanos en términos más familiares que individuales, es decir, no como un conjunto de personas, sino como un conjunto de hermandades, donde una hermandad consta de todas las personas que comparten el mismo padre. En este sentido las relaciones son instrumentos que sirven para enriquecer la forma en que concebimos un conjunto.

En matemáticas los conjuntos juegan el papel de un terreno o región abstracta conformada por elementos que no tienen ningún orden en especial y en donde ningún elemento en principio es más importante o fundamental que otro. Sobre este terreno los elementos se pueden "comparar", "ordenar", etc., y la forma de lograr esto es mediante las relaciones. Éstas dotan de estructura al conjunto en cuestión y establecen conexiones entre sus elementos y subconjuntos.

En este capítulo estudiaremos las relaciones en general, la funciones (que son un caso particular de las relaciones) y las relaciones de equivalencia. Estas herramientas son fundamentales para el desarrollo matemático, pues permiten describir fenómenos estructurales en forma precisa, definir estructuras numéricas importantes —como los enteros, los enteros módulo n, los racionales, los reales y los complejos—, construir objetos geométricos y espaciales, definir con precisión la noción de "isomorfismo entre estructuras" y otras nociones similares, y contar el número de objetos que cumplen cierta propiedad.

§ 4.1 Relaciones

Por simplicidad, en este libro estudiaremos únicamente relaciones *binarias*, es decir, aquellas en donde la conexión se da entre dos objetos. Un ejemplo de ellas es la relación R que ocurre entre personas y libros, por la cual una persona p y un libro l se encuentran "R-relacionados" si y sólo si *p ha leído el libro l*. Podemos abreviar la afirmación "p y l se encuentran R-relacionados" de modo natural, así: pRl.

Esto sugiere que p y l se encuentran conectados por la relación R. Diremos que R es una relación *entre* los conjuntos H y L, esto es, los conjuntos de todos los seres humanos y de todos los libros, respectivamente.

Lo anterior parece sugerir que la relación R no es un objeto tal y como p y l lo son. Sin embargo, hay una manera de "identificar" a R con un objeto—más precisamente, con un conjunto. Esto no debe sorprendernos, pues un conjunto es un objeto que representa cierta *información* al tener o no ciertos elementos. En nuestro caso, conocer la relación R consiste en conocer dos cosas, a saber:

(a) Los dos conjuntos entre los cuales se da la relación. En este caso, H y L, seres humanos y libros.

(b) El conjunto de todas las parejas relacionadas por la relación R, es decir, aquéllas formadas por una persona y un libro que ha leído: (John Benavides, *El extranjero*), (Verónica Mariño, *El Quijote*), (Julián Castillo, *La metamorfosis*), (Nelson Gasca, *Don Juan*), etc.

Naturalmente, el conjunto de todas las parejas relacionadas por la relación R nos da, por sí solo, la información esencial sobre esta relación. De este modo *identificamos* a R con el conjunto de parejas relacionadas por la relación que tenemos en mente:

$$R = \{ (p,l) : p \text{ es un ser humano, } l \text{ es un libro y } p \text{ ha leído a } l \};$$

o, lo que es igual,

$$R = \{ (p,l) \in H \times L : p \text{ ha leído a } l \}.$$

La afirmación "pRl" será entonces una abreviación de "$(p,l) \in R$". Una vez más, la noción de pertenencia sirve para fundamentar y formalizar conceptos más complejos.[1]

Evidentemente preguntarse cuáles son todas las posibles relaciones entre H y L equivale a preguntarse cuáles son todos los posibles conjuntos de parejas de la forma (p,l), donde $p \in H$ y $l \in L$. Concluimos que el conjunto de todas las relaciones entre H y L es $\mathcal{P}(H \times L)$. Las consideraciones anteriores motivan la definición formal de una relación:

Definición 4.1 (Relación). Sean A y B conjuntos. Una *relación* entre A y B es un subconjunto de $A \times B$, esto es, un conjunto R tal que $R \subseteq A \times B$. *Relación*

Por conveniencia, si R es una relación entre A y A, diremos que R es una relación *sobre* A. Por ende, el conjunto de relaciones sobre A es

$$\mathcal{P}(A \times A) = \mathcal{P}(A^2).$$

Veamos ahora algunos ejemplos de relaciones:

Ejemplo 4.2. Sea R la relación que corresponde a la figura de abajo. Entonces R es el conjunto de los siguientes pares ordenados:

$$R = \{(b,1),(c,1),(c,4),(d,3)\} \subseteq A \times B.$$

El elemento c se relaciona simultáneamente con dos objetos distintos y el elemento a no se relaciona con ningún objeto. Note que no es correcto decir que 1 se relaciona con c, sino más bien que c se relaciona con 1. Por esto utilizamos flechas y no líneas como conexiones en el dibujo.

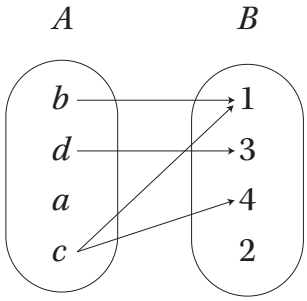


Figura 4.1 : Representación esquemática de la relación R.

[1] Recordemos, por ejemplo, que la noción de ser un subconjunto también está definida en términos de la pertenencia.

Ejemplo 4.3 (La relación *ser madre de*). Sea R la relación entre seres humanos *ser madre de*. Esto es, aRb si y sólo si *a es madre de b*. R es una relación sobre H, el conjunto de los seres humanos. Sabemos, por ejemplo, que para todo x se da que $(x,x) \notin R$, pues nadie puede ser su propia madre. Además, si $(x,y) \in R$, entonces $(y,x) \notin R$. Esto ilustra que el concepto de relación no es en general *simétrico*, de modo que al nombrar los objetos que se relacionan importa el orden en que éstos se mencionan. Por supuesto, esto no impide que existan muchas relaciones simétricas como, por ejemplo, la relación *ser hermano de*.

Ejemplo 4.4 (La relación $\leq$). Sea $R = \{(n,m) \in \mathbb{N}^2 : \text{existe } k \in \mathbb{N} \text{ tal que } n+k=m\}$. Es claro que $(n,m) \in R$ si y sólo si $n \leq m$, de modo que $R = \leq$. Entonces $\leq$ es el subconjunto de $\mathbb{N}^2$ que contiene las parejas $(0,0),(0,1),(1,4),(10,23),(6,6)$, etc. Una forma más precisa de describir esta relación es la siguiente:

$$\leq = \bigcup_{n\in\mathbb{N}} \{n\} \times \mathbb{N}^{\geq n}.$$

☞ **Antes de seguir leyendo**

Identifique las siguientes relaciones conocidas sobre $\mathbb{N}$:

1. $R = \bigcup_{n\in\mathbb{N}^*} (\{n\} \times \{0,\ldots,n-1\})$;
2. $R = \bigcup_{n\in\mathbb{N}} (\{n\} \times \{n\})$;
3. $R = \bigcup_{n\in\mathbb{N}^*} (\{n\} \times \{n,2n,3n,\ldots\})$.

Ejemplo 4.5 (La relación vacía). Dado que $\varnothing \subseteq A \times B$, por definición tenemos que $\varnothing$ es una relación, la cual se denomina *relación vacía*. Bajo esta relación ningún elemento se relaciona con ningún otro.

Ejemplo 4.6 (La relación identidad). Dado un conjunto A, definimos la relación $\text{ID}_A := \{(x,x) : x \in A\}$. En otras palabras, $a \,\text{ID}_A\, b$ si y sólo si $a = b$. Note que $\text{ID}_A \subseteq A^2$.

Ejemplo 4.7 (La relación $\subseteq$). Dado un conjunto A, definimos la relación S_A sobre $\mathcal{P}(A)$ así:

$$BS_AC \text{ si y sólo si } B \subseteq C.$$

Es decir,

$$S_A = \{(B, C) \in \mathcal{P}(A) \times \mathcal{P}(A) : B \subseteq C\}.$$

La relación S_A se llama la *relación* $\subseteq$ *restringida a* $\mathcal{P}(A)$. Observe que $\varnothing$ está S_A-relacionado con todos los subconjuntos de A y todos los subconjuntos de A están S_A-relacionados con A. De modo que, coloquialmente hablando, la relación S_A tiene siempre un "piso" ($\varnothing$) y un "techo" (A).

Ahora definimos las nociones de *dominio*, *imagen* y *campo* de una relación:

Definición 4.8. Definimos los siguientes conjuntos asociados a R:

(a) El *dominio* de R, $\textsc{dom}(R) := \{x : \text{ existe } y \text{ tal que } (x, y) \in R\}$. *Dominio*

(b) La *imagen* de R, $\textsc{img}(R) := \{y : \text{ existe } x \text{ tal que } (x, y) \in R\}$. *Imagen*

(c) El *campo* de R, $\textsc{cmp}(R) := \textsc{dom}(R) \cup \textsc{img}(R)$. *Campo*

Ejemplo 4.9. Sea $R = \{(1, 2), (3, 2), (1, 0), (a, t), (4, 4), (5, b)\}$. Entonces se tiene:

(a) $\textsc{dom}(R) = \{1, 3, 4, 5, a\}$.

(b) $\textsc{img}(R) = \{0, 2, 4, b, t\}$.

(c) $\textsc{cmp}(R) = \{0, 1, 2, 3, 4, 5, a, b, t\}$.

Para toda relación R, $R \subseteq \textsc{dom}(R) \times \textsc{img}(R)$ y $R \subseteq \textsc{cmp}(R)^2$, de modo que toda relación puede verse como un subconjunto de C^2 para un conjunto C, que no es único. Esto es, no perdemos generalidad al considerar únicamente relaciones sobre un conjunto.

☞ **Antes de seguir leyendo**

Sea R una relación y sea $C = \textsc{cmp}(R)$. Demuestre que C es el *mínimo* conjunto X tal que $R \subseteq X^2$. Esto es, $R \subseteq C^2$ y $\forall X : R \subseteq X^2 \to C \subseteq X$.

Definición 4.10. Sean R una relación y A un conjunto. Definimos los siguientes conjuntos:

$R[A]$: Imagen de A bajo R

(a) La *imagen* de A bajo R,

$$R[A] := \{y \in \text{IMG}(R) : \text{ existe } x \in A \text{ tal que } (x,y) \in R\}.$$

$R^{-1}[A]$: Preimagen de A bajo R

(b) La *preimagen* o *imagen inversa* de A bajo R,

$$R^{-1}[A] := \{x \in \text{DOM}(R) : \text{ existe } y \in A \text{ tal que } (x,y) \in R\}.$$

Ejemplo 4.11. Sea $M = \{(z,-z) : z \in \mathbb{Z}\}$. Tenemos:

(a) $M[\{0\}] = \{0\}$.
(b) $M[\mathbb{Z}^-] = \mathbb{Z}^+$.
(c) $M^{-1}[\{1,2,3,4\}] = \{-1,-2,-3,-4\}$.
(d) $M[2\mathbb{Z}] = 2\mathbb{Z}$.
(e) $M[\{\pi, 2\pi\}] = \varnothing$.

Ejemplo 4.12. Sea $T = \{(|z+1|, z) : z \in \mathbb{R}\}$. Así, por ejemplo, $(|-5+1|, -5) = (4,-5) \in T$ y $(|3+1|, 3) = (4,3) \in T$. Tenemos:

(a) $T[\{1\}] = \{-2, 0\}$; $T^{-1}[\{2\}] = \{3\}$.
(b) $T[\mathbb{N}] = \mathbb{Z}$.
(c) La imagen del conjunto de los pares bajo T es el conjunto de los impares, y la imagen del conjunto de los impares bajo T es el conjunto de los pares.
(d) La preimagen del conjunto de los pares bajo T es el conjunto de los impares positivos. La imagen del conjunto de los enteros negativos bajo T es igual al conjunto vacío. Esto vale ya que $|z+1|$ nunca es negativo.

El siguiente teorema establece las relaciones básicas entre los conceptos de dominio, imagen, imagen de un conjunto y preimagen de un conjunto:

Teorema 4.13. Sea R una relación y sean A y B conjuntos tales que $A \subseteq \text{DOM}(R)$ y $B \subseteq \text{IMG}(R)$. Tenemos:

(a) $A \subseteq R^{-1}[R[A]]$;

(b) $B \subseteq R[R^{-1}[B]]$;

(c) $R[\text{DOM}(R)] = \text{IMG}(R)$;

(d) $R^{-1}[\text{IMG}(R)] = \text{DOM}(R)$.

Prueba. Demostramos (a) y (d) y dejamos la prueba de las demás propiedades al lector (ejercicio 4).

(a) Sea $a \in A$. Como $A \subseteq \text{DOM}(R)$, entonces $a \in \text{DOM}(R)$. Luego existe b tal que $(a,b) \in R$. Entonces, por definición de $R[A]$, concluimos que $b \in R[A]$. Como $(a,b) \in R$ y $b \in R[A]$, concluimos por definición que $a \in R^{-1}[R[A]]$.

(d) Utilizamos el método de doble inclusión:

(⊆) Sea $a \in R^{-1}[\text{IMG}(R)]$. Entonces, por la Definición 4.10, existe $b \in \text{IMG}(R)$ tal que $(a,b) \in R$. Esto implica que $a \in \text{DOM}(R)$.

(⊇) Sea $a \in \text{DOM}(R)$. Entonces, por la Definición 4.10, existe b tal que $(a,b) \in R$. Esto implica que $b \in \text{IMG}(R)$. Ahora, debido a que $(a,b) \in R$ y $b \in \text{IMG}(R)$, podemos concluir, por definición, que $a \in R^{-1}[\text{IMG}(R)]$. ∎

Dada una relación R, definimos su *inversa*, R^{-1}, así:

Definición 4.14 (Relación inversa). Dada una relación R, su *inversa* es la relación dada por $R^{-1} := \{(y,x) : (x,y) \in R\}$. En otras palabras, $aR^{-1}b$ si y sólo si bRa.

R^{-1}: Relación inversa

Por ejemplo, la relación inversa de la relación *ser mayor* es la relación *ser menor*, y la relación inversa de la relación *ser hermano o hermana* es ella misma. La relación inversa de la relación *es múltiplo de* es la relación *divide a*.

> ☞ **Antes de seguir leyendo**
>
> Sea R una relación. Demuestre las siguientes igualdades:
>
> 1. $\text{DOM}(R^{-1}) = \text{IMG}(R)$; 2. $\text{IMG}(R^{-1}) = \text{DOM}(R)$.

Hemos creado, de una forma sutil, un pequeño problema de notación: $R^{-1}[A]$ denota, por una parte, la preimagen de A bajo R y, por otra, la imagen de A bajo la relación R^{-1}. El siguiente lema muestra que los dos conjuntos anteriores coinciden en general; de esta forma eliminamos cualquier posibilidad de ambigüedad:

Lema 4.15. Sea R una relación y A un conjunto. Entonces la preimagen de A bajo R es igual a la imagen de A bajo R^{-1}.

Prueba. Sean P la preimagen de A bajo R e I la imagen de A bajo la relación R^{-1}. Debemos probar que $P = I$. Para cualquier x vale lo siguiente:

$$\begin{aligned} x \in P &\leftrightarrow \exists y \in A : (x,y) \in R \\ &\leftrightarrow \exists y \in A : (y,x) \in R^{-1} \\ &\leftrightarrow x \in I. \end{aligned}$$

La segunda equivalencia vale ya que $(x,y) \in R$ si y sólo si $(y,x) \in R^{-1}$. Concluimos que P e I tienen los mismos elementos. En consecuencia, $P = I = R^{-1}[A]$. ∎

Órdenes

Antes de hablar de las relaciones de orden, conviene examinar qué propiedades puede tener una relación cualquiera.

Definición 4.16 (Propiedades de las relaciones). Sea R una relación sobre un conjunto X. Diremos que R es:

(a) *reflexiva sobre* X, si $\forall a \in X$: $(a,a) \in R$;
(b) *irreflexiva sobre* X, si $\forall a \in X$: $(a,a) \notin R$;
(c) *simétrica*, si $\forall a,b$:$(a,b) \in R \to (b,a) \in R$;
(d) *asimétrica*, si $\forall a,b$:$(a,b) \in R \to (b,a) \notin R$;
(e) *antisimétrica*, si $\forall a,b$:$[(a,b) \in R \wedge (b,a) \in R] \to a = b$;
(f) *transitiva*, si $\forall a,b,c$:$[(a,b) \in R \wedge (b,c) \in R] \to (a,c) \in R$.

Ejemplo 4.17. Sea $X = \mathbb{Z}$ y definamos la relación R sobre X de la siguiente forma:

$$(x,y) \in R \text{ si y sólo si } |x| \leq |y|.$$

(a) Esta relación es reflexiva sobre X, pues $\forall x \in X : |x| \leq |x|$.
(b) Esta relación no es simétrica, puesto que $(2,4) \in R$, pero $(4,2) \notin R$.
(c) Esta relación no es antisimétrica, puesto que $(3,-3) \in R$ y $(-3,3) \in R$, pero $3 \neq -3$.

(d) Esta relación es transitiva, puesto que si $(x,y) \in R$ y $(y,z) \in R$, entonces tenemos que $|x| \leq |y|$ y $|y| \leq |z|$; luego $|x| \leq |z|$, lo que implica por definición que $(x,z) \in R$.

☞ **Antes de seguir leyendo**

1. Recuerde que $\varnothing$ es una relación sobre cualquier conjunto A. ¿Qué propiedades de la Definición 4.16 cumple la relación $\varnothing$?
2. Sea X un conjunto cualquiera no vacío. ¿Qué propiedades de la Definición 4.16 cumple la relación ID_X?
3. ¿Cuál es la diferencia entre las propiedades *ser asimétrica*, *no ser simétrica* y *ser antisimétrica*? Dé un ejemplo de una relación simétrica y antisimétrica. Dé un ejemplo de una relación antisimétrica que no sea asimétrica.

Dado que una relación es un conjunto (de parejas ordenadas), es natural hablar de la unión e intersección entre dos relaciones. Por ejemplo, sea $X = \{1,2,3,4\}$ y sean R y S las siguientes relaciones sobre X:

$$R = \{(1,2),(2,1),(2,3),(4,4)\},$$
$$S = \{(1,2),(3,2),(1,4),(3,3),(4,4)\}.$$

Entonces $R \cup S$ es la relación:

$$R \cup S = \{(1,2),(1,4),(2,1),(2,3),(3,2),(3,3),(4,4)\},$$

mientras que $R \cap S$ es la relación:

$$R \cap S = \{(1,2),(4,4)\}.$$

En el siguiente teorema demostraremos que la operación de intersección preserva ciertas propiedades de las relaciones, en el sentido de que si dos relaciones comparten una propiedad, entonces su intersección también poseerá esta propiedad.

Teorema 4.18. Sea X un conjunto y sean R y S relaciones sobre X, esto es, $R, S \subseteq X^2$. Entonces:

(a) Si R y S son reflexivas sobre X, entonces la relación $R \cap S$ es reflexiva sobre X.

(b) Si R y S son simétricas, entonces la relación $R \cap S$ es simétrica.

(c) Si R y S son transitivas, entonces la relación $R \cap S$ es transitiva.

Prueba.

(a) Sea $a \in X$. Por hipótesis, R y S son reflexivas, luego $(a,a) \in R$ y $(a,a) \in S$. Entonces tenemos que $(a,a) \in R \cap S$, como queríamos.

(b) Sean $a,b \in X$ y supongamos que $(a,b) \in R \cap S$. Por la definición de intersección, lo anterior implica que $(a,b) \in R$ y $(a,b) \in S$. Como R y S son simétricas, entonces $(b,a) \in R$ y $(b,a) \in S$. Luego, por definición de intersección, $(b,a) \in R \cap S$.

(c) Sean $a,b,c \in X$ y supongamos que

$$(a,b) \in R \cap S \text{ y } (b,c) \in R \cap S.$$

Entonces $(a,b) \in R$, $(b,c) \in R$, $(a,b) \in S$ y $(b,c) \in S$. Por hipótesis R y S son relaciones transitivas, luego $(a,c) \in R$, y $(a,c) \in S$. Esto implica que $(a,c) \in R \cap S$, como se quería demostrar. ∎

En el ejercicio 11 se pedirá determinar qué propiedades preserva en general la unión entre dos relaciones.

Recordemos los conceptos básicos sobre órdenes. Por definición un *orden parcial* sobre X es una relación $R \subseteq X^2$ que es reflexiva sobre X, antisimétrica y transitiva. Usualmente se utiliza el símbolo $\leq$ para referirse a órdenes parciales. Si $\leq$ es un orden parcial sobre X, diremos que $(X,\leq)$ es una *estructura parcialmente ordenada*.

Si $\leq$ es un orden parcial sobre X, simbolizamos por $<$ a la relación sobre X definida así:

$$a < b \text{ si y sólo si } a \leq b \text{ y } a \neq b.$$

Diremos que $<$ es el *orden parcial estricto* sobre X asociado al orden parcial $\leq$. Conjuntistamente tenemos que $< = \leq \setminus \mathrm{ID}_X$. Se tiene que $<$ es una relación irreflexiva sobre X, asimétrica y transitiva.

Además, $\geq$ y $>$ son las relaciones inversas de $\leq$ y $<$ respectivamente. Conjuntistamente, $\geq := \leq^{-1}$ y $> := <^{-1}$.

Recordemos ahora la definición de un *orden lineal*:

Definición 4.19. Sea $\leq$ una relación sobre X. Diremos que $\leq$ es un *orden lineal* sobre X, o que X es un conjunto linealmente ordenado por $\leq$, si:

Orden lineal

(a) $\leq$ es un orden parcial sobre X; y

(b) $\leq$ es total sobre X, es decir, dados a y $b \in X$, entonces $a \leq b$ o $b \leq a$.

Orden total Por definición, un *orden total* es un orden lineal.

En otras palabras, un orden total es un orden parcial en el cual todos los elementos son *comparables* (propiedad (b)). Equivalentemente, un orden total es un orden parcial $\leq$ cuyo orden estricto asociado $<$

cumple la siguiente propiedad, llamada *tricotomía*: dados $a, b \in X$ vale *exclusivamente* una de las tres afirmaciones siguientes: *Tricotomía*

$$a < b; \quad a = b; \quad a > b.$$

Hasta ahora hemos estudiado con cierto detalle los órdenes parciales de contenencia $(\mathcal{P}(\mathcal{U}), \subseteq)$ y divisibilidad $(\mathbb{N}^*, |)$. Además, hemos estudiado el orden usual en los números naturales y en los enteros, $(\mathbb{N}, \leq), (\mathbb{Z}, \leq)$, los cuales son órdenes lineales. La relación de congruencia módulo n $(\mathbb{Z}, \equiv_n)$, que consideramos en el capítulo 3, no es un orden parcial, ya que no es antisimétrica. Esta relación será un ejemplo fundamental de las llamadas *relaciones de equivalencia*, que estudiaremos más adelante.

Ahora definimos los conceptos de *cota inferior*, *mínimo*, *minimal* e *ínfimo* de un conjunto:

Definición 4.20. Sea $(X, \leq)$ una estructura parcialmente ordenada y sean $a \in X$ y $S \subseteq X$. Diremos que:

(a) a es *una cota inferior de* S si para todo $s \in S$ tenemos que $a \leq s$. Esto lo denotamos así: $a \leq S$. *Cota inferior*

(b) a es un *mínimo de* S si $a \in S$ y $a \leq S$. *Mínimo*

(c) a es un *minimal de* S si $a \in S$ y no existe $b \in S$ tal que $b < a$. *Minimal*

(d) a es un *ínfimo de* S si $a \leq S$ y para todo x tal que $x \leq S$, entonces $x \leq a$. A tal elemento a se le llama también una *máxima cota inferior de* S, pues es mayor o igual a todas las cotas inferiores de S. *Ínfimo*

Si intercambiamos $\leq$ por $\geq$ en las definiciones (a)–(d) de arriba, podemos definir de forma similar los conceptos de *cota superior*, *máximo*, *maximal* y *supremo* (o *mínima cota superior*) de un conjunto. Por ejemplo, a es un *supremo* de S si $a \geq S$ y para todo x tal que $x \geq S$, entonces $x \geq a$. *Cota superior* *Máximo* *Maximal* *Supremo*

Teorema 4.21. Sea $(X, \leq)$ un conjunto parcialmente ordenado y sean $a, b \in X$ y $S \subseteq X$. Entonces:

(a) Si a y b son mínimos de S, entonces $a = b$.

(b) Si a es mínimo de S, entonces a es minimal e ínfimo de S.

(c) Si a y b son ínfimos de S, entonces $a = b$.

(d) Si $\leq$ es un orden total, entonces a es mínimo de S si y sólo si a es minimal de S.

Prueba. Se deja al lector (ejercicio 10). ∎

Este teorema garantiza que, en un orden parcial $(X, \leq)$, un conjunto $S \subseteq X$ tiene a lo sumo un mínimo y a lo sumo un ínfimo, y que si S

MÍN(S): *mínimo de S*
ÍNF(S): *ínfimo de S*
MÁX(S): *máximo de S*
SUP(S): *supremo de S*

tiene un mínimo, entonces este elemento también será su ínfimo. En estos casos llamaremos MÍN(S) al elemento mínimo de S, e ÍNF(S) al elemento ínfimo de S. Análogamente, si S tiene un elemento máximo, será único y lo denotaremos como MÁX(S); y si S tiene un supremo, también será único y lo denotaremos como SUP(S).

Vale la pena hacer las siguientes observaciones adicionales:

Observación 4.22.

(a) Existen conjuntos S que no tienen elemento mínimo.

(b) Existen conjuntos S que tienen más de un elemento maximal.

(c) Existen conjuntos S que no tienen ínfimo.

(d) Existen conjuntos S que tienen ínfimo pero no tienen mínimo.

Ejemplo 4.23. Sea $X = \mathbb{R}$, con su orden $\leq$ usual. Sean

$S_1 = \mathbb{Z}$, $S_2 = \{1, -2, 5\}$, $S_3 = (2, 4] = \{x \in \mathbb{R} : 2 < x \leq 4\}$, $S_4 = \varnothing$, $S_5 = \mathbb{R}$.

Entonces podemos afirmar que:

(a) S_1 no tiene mínimo, máximo, ínfimo ni supremo.

(b) MÍN(S_2) $= -2$ y MÁX(S_2) $= 5$.

(c) S_3 no tiene mínimo, ÍNF(S_3) $= 2$ y MÁX(S_3) $= 4$.

(d) S_4 no tiene mínimo, máximo, ínfimo ni supremo, pero tiene cotas.

(e) S_5 no tiene mínimo, máximo, ínfimo, supremo ni cotas.

Ejemplo 4.24. Sea X el conjunto de divisores positivos de 24:

$$X = D_{24}^{+} = \{1, 2, 3, 4, 6, 8, 12, 24\}.$$

Sea $S = \{1, 2, 3, 4, 6\}$. Consideremos el orden parcial $(X, |)$. Entonces:

(a) S no tiene máximo.

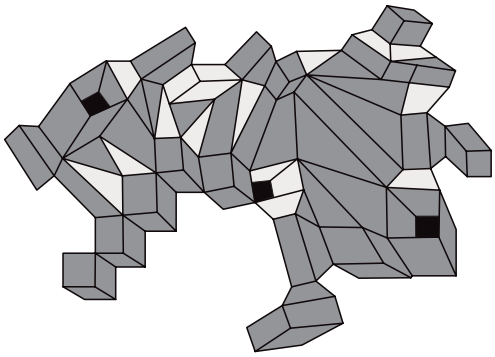
(b) S tiene dos elementos maximales: 4 y 6.

(c) 12 y 24 son cotas superiores de S.

(d) El supremo de S es 12: SUP(S) $= 12$.

(e) 1 es el mínimo y el ínfimo de S. Además, es su único elemento minimal y su única cota inferior.

Ejercicios



1. Para cada una de las siguientes relaciones R, liste todos los elementos de ella:
   (a) $R = \{(a,b) \in \mathbb{Z}^2 : 0 \leq a \leq 5 \text{ y } b = a+2\}$.
   (b) $R = \{(a,b) \in \mathbb{N}^2 : a+b = 9\}$.
   (c) $R = \{(a,b) \in \mathbb{N}^2 : ab = 36\}$.
2. Sea $X = \{1,2,3\}$. Liste todas las relaciones simétricas sobre X.
3. Sea $X = \{1,3,5,7\}$. Liste todas las relaciones sobre X que sean reflexivas, simétricas y transitivas.
4. Demuestre las partes (b) y (c) del Teorema 4.13.
5. Diremos que una relación $R \subseteq X^2$ es *completa* si existe un conjunto $A \subseteq X$ tal que $R = A \times A$. Demuestre que si R es completa, entonces R es simétrica y transitiva.
6. Sea R la siguiente relación sobre $\mathbb{Z}^*$: dados $a, b \in \mathbb{Z}^*$, aRb si y sólo si $ab > 0$. Demuestre que R es reflexiva, simétrica y transitiva.
7. Sea $(X, \leq)$ un conjunto parcialmente ordenado, con $a, a', b \in X$ y $S, S' \subseteq X$. Demuestre que si a es una cota inferior de S, a' es una cota inferior de S' y b es una cota inferior de $\{a, a'\}$, entonces b es una cota inferior de $S \cup S'$.
8. Dé un ejemplo de un orden parcial pero no total $(X, \leq)$, en el cual todo conjunto $S \subseteq X$ tenga una cota inferior y una cota superior.
9. Sea $S = \{\frac{1}{n} : n = 1,2,3,\dots\} \subseteq \mathbb{R}$, dotado del orden usual. Determine el máximo, mínimo, supremo e ínfimo de S, en caso de existir.
10. Demuestre el Teorema 4.21.

11. Sean R y S relaciones sobre X. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:
    (a) Si R y S son reflexivas sobre X, entonces $R \cup S$ también lo es.
    (b) Si R y S son simétricas, entonces $R \cup S$ también lo es.
    (c) Si R y S son antisimétricas, entonces $R \cup S$ también lo es.
    (d) Si R y S son transitivas, entonces $R \cup S$ también lo es.
12. Sea R una relación sobre X.
    (a) Demuestre que R es asimétrica si y sólo si $R \cap R^{-1} = \varnothing$.
    (b) Demuestre que R es antisimétrica si y sólo si $(R \cap R^{-1}) \subseteq \mathrm{ID}_X$.
    (c) Concluya que toda relación asimétrica es antisimétrica, y dé un ejemplo de una relación que sea antisimétrica pero no asimétrica.
13. Dada una relación R sobre X, sean $S(R)$ y $L(R)$ los siguientes conjuntos:
$$S(R) = \{x \in X : \text{para todo } y \in X,\ xRy\},$$
$$L(R) = \{x \in X : \text{para todo } y \in X,\ yRx\}.$$
    Demuestre que $S(R) = L(R^{-1})$ y $S(R^{-1}) = L(R)$.
14. Sea $R \subseteq X^2$. Demuestre que R es reflexiva sobre X si y sólo si R^c es irreflexiva sobre X. (Aquí $R^c := X^2 \setminus R$.)
15. Demuestre que si R es una relación simétrica y transitiva entonces $R \circ R$ es simétrica y transitiva. (La relación $R \circ R$ se define así: $\{(a,c) :$ existe b tal que $(a,b) \in R$ y $(b,c) \in R\}$; cf. § 4.3, abajo.)
16. Sea $R \subseteq X^2$ una relación simétrica. Demuestre que $R^c = X^2 \setminus R$ es una relación simétrica.
17. Sea R una relación sobre X y S una relación sobre Y. Definimos la siguiente relación T sobre $X \times Y$:
$$(x,y)T(x',y') \leftrightarrow [xRx' \wedge ySy'].$$
    Note que T es una relación *entre pares ordenados*. Conjuntistamente tenemos que $T \subseteq (X \times Y) \times (X \times Y)$. Demuestre las siguientes afirmaciones:
    (a) Si R es irreflexiva sobre X y S es irreflexiva sobre Y, entonces T es irreflexiva sobre $X \times Y$.
    (b) Si R y S son antisimétricas, entonces T es antisimétrica.
    (c) $\mathrm{DOM}(T) = \mathrm{DOM}(R) \times \mathrm{DOM}(S)$.
    (d) $\mathrm{IMG}(T) = \mathrm{IMG}(R) \times \mathrm{IMG}(S)$.

18. Para todo $n \in \mathbb{N}$ sea R_n una relación. Demuestre que es el caso que $\bigcap_{n\in\mathbb{N}} R_n^{-1} = \left(\bigcap_{n\in\mathbb{N}} R_n\right)^{-1}$. ¿Se obtiene el mismo resultado si cambiamos $\bigcap$ por $\bigcup$?
19. Dado un conjunto X y $S \subseteq X$, sea $R_S = \{(A,B) \in \mathcal{P}(X)^2 : A \cup B^c \subseteq S\}$. (Aquí $B^c = X \setminus B$.)
    (a) ¿Qué conjunto es $\text{DOM}(R_S)$? ¿Qué conjunto es $\text{IMG}(R_S)$?
    (b) Demuestre que si $\text{DOM}(R_S) \cap \text{IMG}(R_S) \neq \varnothing$, entonces $S = X$.
    (c) Dados $S, T \subseteq X$, ¿cómo se comparan $R_{S\cap T}$ y $R_S \cap R_T$?
    (d) Dados $S, T \subseteq X$, ¿cómo se comparan $R_{S\cup T}$ y $R_S \cup R_T$?

§ 4.2 Clausura de una relación

Imaginemos una relación cualquiera R sobre un conjunto X. Supongamos que nos interesa transformar a R en una relación reflexiva sobre X, añadiendo, de ser necesario, más elementos a la relación; en otras palabras, *extendiéndola*.

Por ejemplo, sea $X = \{0,1,2,3\}$ y sea R la siguiente relación sobre X:

$$R = \{(1,2),(3,3),(0,0),(2,3)\}.$$

Para que R sea reflexiva sobre un conjunto X, debemos agregarle los elementos $(1,1)$ y $(2,2)$. Esto es, la relación $S = R \cup \{(1,1),(2,2)\}$ es una *extensión reflexiva de R*, es decir, $S \supseteq R$ y S es reflexiva sobre X. Además, es claro que S es la *mínima* relación reflexiva sobre X que contiene a R en el siguiente sentido:

> Para toda relación T, si T es una relación reflexiva sobre X, y $T \supseteq R$, entonces $T \supseteq S$.

El ejemplo anterior ilustra lo que quisiéramos hacer con una relación: agregar el mínimo número de elementos para que se transforme en una relación con cierta propiedad $\star$, donde $\star$ representa reflexividad, simetría o transitividad. Este proceso se denomina *cerrar* una relación.

Clausuras de una relación

Definición 4.25 (Clausuras de una relación). Sea R una relación sobre un conjunto X. Definimos las siguientes relaciones sobre X:

(a) La *clausura reflexiva* de R es la relación

$$\overline{R}_{\text{REF}} := \bigcap \{S \subseteq X^2 : S \text{ es reflexiva sobre } X \text{ y } S \supseteq R\}.$$

(b) La *clausura simétrica* de R es la relación

$$\overline{R}_{\text{SIM}} := \bigcap \{S \subseteq X^2 : S \text{ es simétrica y } S \supseteq R\}.$$

(c) La *clausura transitiva* de R es la relación

$$\overline{R}_{\mathrm{TR}} := \bigcap \{S \subseteq X^2 : S \text{ es transitiva y } S \supseteq R\}.$$

Note que $\overline{R}_{\mathrm{REF}} \supseteq R$. Luego la clausura reflexiva de R es siempre una extensión de R; lo mismo vale, claro está, para $\overline{R}_{\mathrm{SIM}}$ y $\overline{R}_{\mathrm{TR}}$. Además, veamos que las clausuras cumplen con la propiedad de minimalidad que pretendemos que tengan:

Teorema 4.26. Sea R una relación sobre X.

(a) $\overline{R}_{\mathrm{REF}}$ es la mínima relación reflexiva que contiene a R. En otras palabras, $\overline{R}_{\mathrm{REF}}$ es reflexiva y para toda relación S que sea reflexiva sobre X, si $R \subseteq S$, entonces $\overline{R}_{\mathrm{REF}} \subseteq S$.

(b) $\overline{R}_{\mathrm{SIM}}$ es la mínima relación simétrica que contiene a R.

(c) $\overline{R}_{\mathrm{TR}}$ es la mínima relación transitiva que contiene a R.

Prueba. Demostramos (a) y (b), y dejamos (c) al lector (ejercicio 6).

(a) Para ver que $\overline{R}_{\mathrm{REF}}$ es reflexiva, sea $a \in X$. Entonces para toda relación S reflexiva sobre X, $(a,a) \in S$, es decir,

$$(a,a) \in \bigcap \{S \subseteq X^2 : S \text{ es reflexiva sobre } X \text{ y } S \supseteq R\} = \overline{R}_{\mathrm{REF}}.$$

Ahora demostramos la minimalidad: sea T una relación reflexiva que contiene a R. Entonces, por el Teorema 1.45 (b), se tiene que

$$T \supseteq \bigcap \{S \subseteq X^2 : S \text{ es reflexiva sobre } X \text{ y } S \supseteq R\} = \overline{R}_{\mathrm{REF}}.$$

(b) Veamos primero que $\overline{R}_{\mathrm{SIM}}$ es simétrica: sea $(a,b) \in \overline{R}_{\mathrm{SIM}}$. Entonces para toda relación $S \subseteq X^2$ tal que $R \subseteq S$ y S es simétrica, tenemos que $(a,b) \in S$. Esto implica que para toda $S \subseteq X^2$ tal que S es simétrica y $R \subseteq S$, $(b,a) \in S$. Entonces $(b,a) \in \overline{R}_{\mathrm{SIM}}$. Ahora demostramos la minimalidad: sea $T \subseteq X^2$ una relación simétrica que contiene a R. Entonces, de nuevo por el Teorema 1.45 (b), se tiene que

$$T \supseteq \bigcap \{S : S \subseteq X^2 \text{ es simétrica y } S \supseteq R\} = \overline{R}_{\mathrm{SIM}}. \qquad \blacksquare$$

Teorema 4.27. Sea R una relación sobre X. Entonces se tiene que, para $\star \in \{\mathrm{REF}, \mathrm{SIM}, \mathrm{TR}\}$, R tiene la propiedad $\star$ si y sólo si $\overline{R}_\star = R$.

Prueba. Utilizamos el método de doble implicación:

($\rightarrow$) Si R tiene la propiedad $\star$, entonces claramente R es la mínima relación con la propiedad $\star$ que contiene a R; así que $R = \overline{R}_\star$, por el Teorema 4.26.

($\leftarrow$) Esta implicación es clara, debido a que $\overline{R}_\star$ tiene la propiedad $\star$ (Teorema 4.26). $\blacksquare$

Por ejemplo, la clausura transitiva de una relación transitiva es ella misma. Del teorema anterior puede deducirse el siguiente resultado:

Corolario 4.28. Sea R una relación sobre X. Entonces se tiene que, para $\star \in \{\text{REF}, \text{SIM}, \text{TR}\}$, $\overline{(\overline{R}_\star)}_\star = \overline{R}_\star$.

Prueba. Se deja al lector (ejercicio 7). ∎

Ejemplo 4.29. Sea $X = \{1,2,3,4,5,6,7,8,9\}$ y sea $R \subseteq X^2$ la relación

$$R = \{(1,1),(2,3),(3,1),(3,6),(4,4),(5,2),(7,1),(8,3)\}.$$

A partir de Teorema 4.26 vemos que para construir $\overline{R}_{\text{REF}}$ basta con agregar a R todos los elementos de la forma (a,a), con $a \in X$, que no se encuentran en R:

$$\overline{R}_{\text{REF}} = R \cup \{(2,2),(3,3),(5,5),(6,6),(7,7),(8,8),(9,9)\}.$$

De forma análoga puede verse que para construir $\overline{R}_{\text{SIM}}$ basta con agregar a R todos los elementos de la forma (b,a), tales que no se encuentran en R y que $(a,b) \in R$:

$$\overline{R}_{\text{SIM}} = R \cup \{(3,2),(1,3),(6,3),(2,5),(1,7),(3,8)\}.$$

El caso de la clausura transitiva es el más interesante. Por ejemplo, dado que $(2,3),(3,1) \in R$, entonces $(2,1)$ debe pertenecer a la clausura transitiva de R. Pero como $(5,2) \in R$, entonces el elemento $(5,1)$ *también* debe pertenecer a la clausura transitiva de R. Siguiendo con este razonamiento, el lector puede verificar que

$$\overline{R}_{\text{TR}} = R \cup \{(2,1),(2,6),(5,1),(5,3),(5,6),(8,1),(8,6)\}.$$

En la Figura 4.2 se representan las diferentes relaciones consideradas en este ejemplo. Note que en particular, la clausura simétrica es, visualmente, simétrica con respecto a la diagonal principal.

Las definiciones de $\overline{R}_\star$ son relativamente complejas. A continuación estudiamos ciertas caracterizaciones más simples que es posible dar de ellas, por lo menos en el caso de la reflexividad y la simetría.

Teorema 4.30 (Caracterización de las clausuras). Sea R una relación sobre X. Entonces:

(a) $\overline{R}_{\text{REF}} = R \cup \text{ID}_X$;
(b) $\overline{R}_{\text{SIM}} = R \cup R^{-1}$;

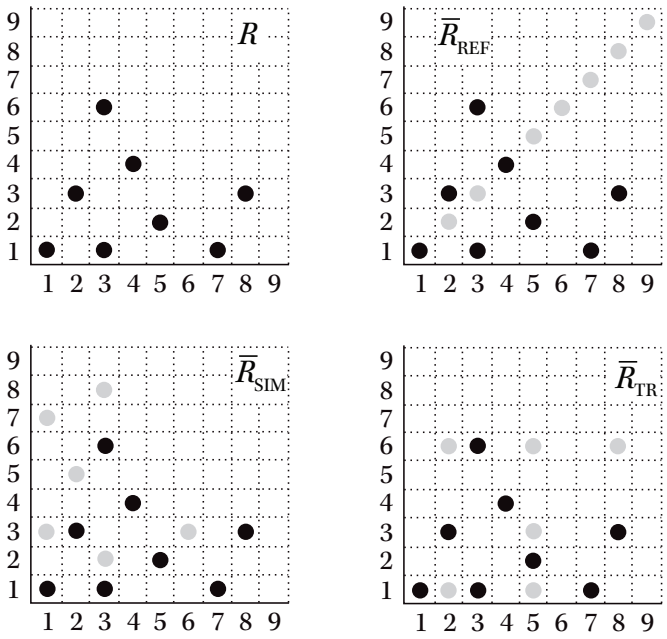


Figura 4.2: Clausuras de la relación R (ejemplo 4.29).

(c) $\overline{R}_{\text{TR}} = \bigcup_{n\in\mathbb{N}^*} R^{(n)}$, en donde $R^{(n)}$ es el conjunto de todos los pares (a,b) tales que existen $a_1, a_2, \ldots, a_n, a_{n+1} \in X$ que cumplen lo siguiente:

(i) $a_1 = a$, $a_{n+1} = b$;

(ii) para $1 \leq i \leq n$, $(a_i, a_{i+1}) \in R$.

Prueba. Dejaremos (b) al lector (ejercicio 8) y demostramos (a) y (c):

(a) Dado $x \in X$, $(x,x) \in R \cup \text{ID}_X$ y $R \subseteq R \cup \text{ID}_X$. Luego $R \cup \text{ID}_X$ es una relación reflexiva sobre X que contiene a R. Por consiguiente, $\overline{R}_{\text{REF}} \subseteq R \cup \text{ID}_X$. Para la otra inclusión, basta observar que si T es una relación reflexiva que contiene a R, entonces $R \cup \text{ID}_X \subseteq T$. Por el Teorema 1.45 (c), concluimos que

$$R \cup \text{ID}_X \subseteq \bigcap \{S \subseteq X^2 : S \text{ es reflexiva y } S \supseteq R\} = \overline{R}_{\text{REF}}.$$

(b) Sea $R' = \bigcup_{n\in\mathbb{N}^*} R^{(n)}$, donde cada R_n se define como en el enunciado del teorema. Debemos demostrar que $\overline{R}_{\text{TR}} = R'$. Utilizamos el método de doble inclusión:

(⊆) Para esta inclusión basta demostrar que R' es una relación transitiva que contiene a R: si $(a,b),(b,c) \in R'$, entonces existen $n,m \in \mathbb{N}^*$ tales que $(a,b) \in R^{(n)}$, $(b,c) \in R^{(m)}$. Por ende, existen $d_2,\dots,d_n$, $e_2,\dots,e_m \in X$ tales que

$$(a,d_2),(d_2,d_3),\dots,(d_n,b),(b,e_2),(e_2,e_3),\dots(e_n,c) \in R.$$

Lo anterior implica por definición que

$$(a,c) \in R^{(n+m)} \subseteq R'.$$

Luego $(a,c) \in R'$. Esto prueba que R' es una relación transitiva. Es claro, a partir de la definición, que $R_1 = R$. Luego $R \subseteq R'$.

(⊇) Para demostrar esta inclusión basta demostrar que para toda relación T sobre X que sea transitiva y contenga a R, $R' \subseteq T$: sea T una relación con las anteriores propiedades. Se deja al lector la tarea de demostrar que para todo $n \in \mathbb{N}^*$ se tiene que $R^{(n)} \subseteq T$ (ejercicio 8). Entonces

$$R' = \bigcup_{n\in\mathbb{N}^*} R^{(n)} \subseteq T.$$

La inclusión vale por el Teorema 1.49. ∎

Ejemplo 4.31. Sea R la relación sobre $\mathbb{Z}$ definida como

$$aRb \text{ si y sólo si } |a-b| = 2,$$

y sea S la mínima relación transitiva sobre $\mathbb{Z}$ que contiene a R, esto es, $S = \overline{R}_{\text{TR}}$. Demuestre que S es precisamente E, la *relación de congruencia módulo 2*, es decir que $\forall a,b \in \mathbb{Z} : (a,b) \in S \leftrightarrow 2 \mid b-a$.

Solución. Primero demostremos que para toda relación transitiva T sobre $\mathbb{Z}$ que contenga a R, se tiene que

$$\forall b \in \mathbb{Z} : \forall n \in \mathbb{N} : [(b,b+2n) \in T \wedge (b,b-2n) \in T].$$

Para ello hacemos inducción en n:

(a) Caso base ($n = 0$): es claro por definición de R que $(b,b+2) \in R$ y, además, que $(b+2,b) \in R$. Entonces $(b,b+2),(b+2,b) \in T$. Como T es transitiva, concluimos que $(b,b) \in T$.

(b) Paso inductivo: supongamos que la afirmación es cierta para n y la demostramos para $n+1$: por hipótesis de inducción, $(b,b+2n) \in T$. Claramente $(b+2n,b+2n+2) \in R \subseteq T$, luego $(b+2n,b+2(n+1)) \in T$. Por transitividad de T concluimos que $(b,b+2(n+1)) \in T$. La demostración de que $(b,b-2(n+1)) \in T$ es análoga.

Ahora demostramos que $E = S$. Para ello utilizamos el método de doble inclusión:

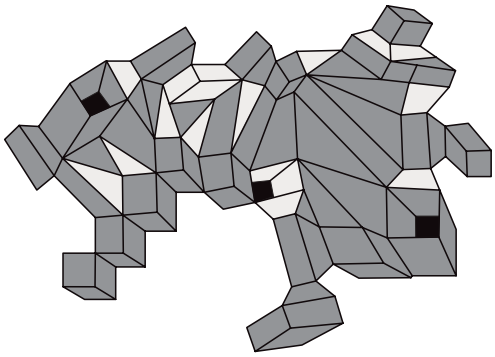
($\subseteq$) Si $(a,b) \in E$, entonces por definición $2 \mid b-a$. Luego existe $n \in \mathbb{Z}$ tal que $b - a = 2n$, y así $b = a + 2n$. Como S es una relación transitiva que contiene a R, la observación anterior garantiza que $(a, a+2n) \in S$, luego $(a,b) \in S$.

($\supseteq$) E es una relación transitiva (Teorema 3.40 (c)) y claramente $R \subseteq E$. Luego por definición de S tenemos que $S \subseteq E$.

Concluimos que $E = S$. ∎

Este ejemplo es sumamente ilustrador. La relación R es bastante *pobre*, pues sólo relaciona puntos que se encuentran a distancia 2. En cambio, su clausura transitiva, E, relaciona puntos a distancia 0, a distancia 2, a distancia 4 y así sucesivamente. Intuitivamente, la relación E *une las piezas de rompecabezas* locales de la relación R, y obtiene así un panorama global que relaciona a dos números enteros según si la distancia entre ellos sea o no par.

Ejercicios



1. Sea $X = \{1,2,3,4,5,6\}$. Para cada una de las siguientes relaciones sobre X, calcule su clausura reflexiva (sobre X), su clausura simétrica y su clausura transitiva:

   (a) $R = \varnothing$.

   (b) $R = \{(1,2),(3,4),(4,5)\}$.

(c) $R = \{(1,2),(2,3),(2,4),(2,5),(6,2)\}$.
(d) $R = \{(1,2),(2,3),(3,4),(4,5),(5,6)\}$.
(e) $R = \{(1,1),(2,3),(3,4),(4,5),(5,2)\}$.

2. Sea $X = \{1,2,3,4\}$ y $R = \{(1,2),(3,4)\}$. Determine el número de relaciones S sobre X tales que $R \subseteq S$ y S es simétrica.
3. Sea $X = \{1,2,3,4\}$ y $R = \{(1,2),(2,3),(2,1)\}$. Determine el número de relaciones S sobre X tales que $R \subseteq S$ y S es transitiva.
4. Para cada una de las siguientes relaciones R sobre $\mathbb{N}$, encuentre las clausuras simétrica y transitiva de R:
   (a) $R = \{(x,y) \in \mathbb{N}^2 : y = x+1\}$.
   (b) $R = \{(x,y) \in \mathbb{N}^2 : x+y = 5\}$.
   (c) $R = \{(x,y) \in \mathbb{N}^2 : x-y = 4\}$.
5. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:
   (a) $\overline{(R \cup S)}_{\text{REF}} = \overline{R}_{\text{REF}} \cup \overline{R}_{\text{REF}}$.
   (b) $\overline{(R \cap S)}_{\text{REF}} = \overline{R}_{\text{REF}} \cap \overline{R}_{\text{REF}}$.
   (c) $\overline{(R \cup S)}_{\text{SIM}} = \overline{R}_{\text{SIM}} \cup \overline{R}_{\text{SIM}}$.
   (d) $\overline{(R \cap S)}_{\text{SIM}} = \overline{R}_{\text{SIM}} \cap \overline{R}_{\text{SIM}}$.
   (e) $\overline{(R \cup S)}_{\text{TR}} = \overline{R}_{\text{TR}} \cup \overline{R}_{\text{TR}}$.
   (f) $\overline{(R \cap S)}_{\text{TR}} = \overline{R}_{\text{TR}} \cap \overline{R}_{\text{TR}}$.
6. Demuestre la parte (c) del Teorema 4.26.
7. Demuestre el Corolario 4.28.
8. Demuestre la parte (b) del Teorema 4.30.
9. Para todo $n \in \mathbb{N}^*$, sea $R^{(n)}$ el conjunto definido como en el enunciado del Teorema 4.30. Sea T una relación sobre X tal que T es transitiva y $R \subseteq T$. Demuestre que para todo $n \in \mathbb{N}^*$, $R^{(n)} \subseteq T$. (*Ayuda*: haga inducción en n.)
10. Sea $X = \mathbb{N}$, y sea $R = \varnothing \subseteq X^2$. Calcule:
    (a) $\overline{R}_{\text{REF}}$, la clausura reflexiva de R (sobre X).
    (b) $\overline{R}_{\text{SIM}}$, la clausura simétrica de R.
    (c) $\overline{R}_{\text{TR}}$, la clausura transitiva de R.
11. Sea R una relación sobre X. Demuestre las siguientes afirmaciones:
    (a) $\text{DOM}(\overline{R}_{\text{REF}}) = \text{IMG}(\overline{R}_{\text{REF}}) = X$.
    (b) $\text{DOM}(\overline{R}_{\text{SIM}}) = \text{IMG}(\overline{R}_{\text{SIM}}) = \text{DOM}(R) \cup \text{IMG}(R)$.
    (c) $\text{DOM}(R) = \text{DOM}(\overline{R}_{\text{TR}})$ e $\text{IMG}(R) = \text{IMG}(\overline{R}_{\text{TR}})$.
12. Definimos la relación R sobre $\mathcal{P}(\mathbb{N})$ de la siguiente manera: dados $S_1, S_2 \in \mathcal{P}(\mathbb{N})$, $(S_1, S_2) \in R$ si y sólo si existe x tal que $S_1 \cup \{x\} = S_2$ o $S_2 \cup \{x\} = S_1$.

(a) Demuestre que R es una relación simétrica.

(b) Sea $S = \overline{R}_{\text{TR}}$. Demuestre que dos conjuntos se encuentran relacionados bajo S si y sólo si es posible obtener un conjunto a partir del otro, primero quitando un número finito (posiblemente 0) de elementos, y luego agregando un número finito (posiblemente 0) de elementos. (De forma equivalente, $(A_1, A_2) \in S$ si y sólo si existen los conjuntos finitos $X_1, X_2 \subseteq \mathbb{N}$ tal que $A_1 \cup X_1 = A_2 \cup X_2$.)

(c) Describa precisamente los elementos del siguiente conjunto:

$$\{A \in \mathcal{P}(\mathbb{N}) : (\varnothing, A) \in S\}.$$

(d) Demuestre que la relación S se encuentra caracterizada así:

$$(A_1, A_2) \in S \leftrightarrow A_1 \triangle A_2 \text{ es un conjunto finito.}$$

13. Demuestre las siguientes afirmaciones:

(a) Si R, S son relaciones sobre X tales que R es reflexiva y $R \subseteq S$, entonces S es reflexiva.

(b) La clausura transitiva de una relación simétrica es simétrica. Dé un ejemplo de una relación transitiva cuya clausura simétrica no sea transitiva.

§ 4.3 Funciones

Intuitivamente una *función* es una regla que asocia elementos de un conjunto con elementos de otro conjunto, de modo que cada elemento del primer conjunto se asocia, o relaciona, *con uno y sólo un elemento* del segundo conjunto. Visto de otro modo, una función es una máquina que transforma cada uno de los elementos x de un conjunto en otro elemento bien definido, y.

Función

Definición 4.32 (Función). Una *función* es una relación f que cumple la siguiente propiedad:

$$\text{si } (x, y) \in f \text{ y } (x, y') \in f, \text{ entonces } y = y'.$$

Es decir, para todo $x \in \text{DOM}(f)$ existe *un único* y tal que $(x, y) \in f$.

Ejemplo 4.33. Considere las relaciones f y g dadas por

$$f = \{(a, y), (b, z), (c, y), (d, w)\};$$
$$g = \{(a, y), (a, z), (b, z), (c, w), (d, w)\}.$$

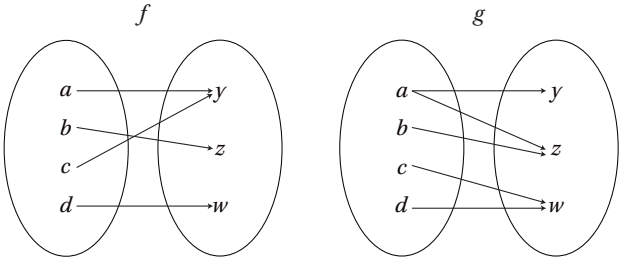


Figura 4.3: Representaciones esquemáticas de f y g.

Se tiene entonces que f es una función cuyo dominio es el conjunto $\{a,b,c,d\}$, mientras que g es una relación que no es función, ya que $(a,y),(a,z) \in g$, pero $y \neq z$.

Ejemplo 4.34 (La función identidad). Dado un conjunto A, la relación ID_A es una función, pues si $(x,y),(x,y') \in \text{ID}_A$, entonces $x = y$ y $x = y'$, luego $y = y'$. Además, $\text{DOM}(\text{ID}_A) = A$.

La relación *divide* $| \subseteq \mathbb{Z}^2$ no es una función, puesto que un número entero puede dividir a más de un número. Por ejemplo, $(2,4) \in |$ y $(2,10) \in |$, pero $4 \neq 10$. La relación definida por xRy si y sólo si "*y es la madre de x*" es una función, pues todo ser humano x tiene una única madre y.

Dada una función f y un elemento x de su dominio, llamaremos $f(x)$ al *único* y tal que $(x,y) \in f$. Por lo tanto, las proposiciones $(x,y) \in f$, xfy y $y = f(x)$ son equivalentes. Note que al utilizar la expresión $f(x)$ se supone implícitamente que $x \in \text{DOM}(f)$. El lector debe ser cuidadoso con esta sutileza. Concluimos que si f es una función, entonces f está dada como conjunto por $f = \{(x, f(x)) : x \in \text{DOM}(f)\}$.

La expresión $f : A \to B$ significará por convención lo siguiente: f es una función, $\text{DOM}(f) = A$ e $\text{IMG}(f) \subseteq B$. Una manera común de describir una función f es especificar su dominio A, dando una definición para $f(x)$ en términos de $x \in A$.

Ejemplo 4.35. Sea f la siguiente función: su dominio es $\mathbb{N}$ y para todo $n \in \mathbb{N}$, $f(n) = -n^2 - 1$. Por ejemplo, $f(0) = -1$, $f(6) = -37$, etc. Ya que, para todo $n \in \mathbb{N}$ tenemos que $f(n) \in \mathbb{Z}^-$, podemos afirmar lo siguiente: $f : \mathbb{N} \to \mathbb{Z}^-$ (se lee: *f es una función de* $\mathbb{N}$ *a* $\mathbb{Z}^-$).

☞ **Antes de seguir leyendo**

Considere la figura de abajo. ¿Cuáles de las relaciones ahí representadas son funciones? Justifique claramente sus respuestas. Determine el dominio y la imagen de f y de g.

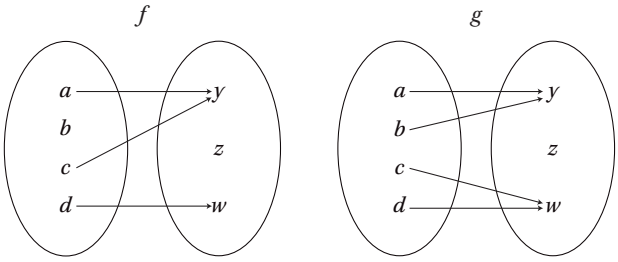


Figura 4.4: Representaciones esquemáticas de la relaciones f y g.

↦: Aplicación

Una manera equivalente de decir $y = f(x)$ es $x \mapsto y$, que se lee *f envía (asocia) x a (con) y*. Por ejemplo, la función

$$\begin{aligned} g : \mathbb{Z}^* &\to \mathbb{Q} \\ z &\mapsto \frac{z}{|z|}, \end{aligned}$$

es la dada por $g(z) = \frac{z}{|z|}$, cuyo dominio es el conjunto de los enteros no nulos. Una descripción conjuntista de g es la siguiente:

$$g = \left\{ (x, y) : x \in \mathbb{Z}^*, y = \frac{x}{|x|} \right\} \subseteq \mathbb{Z}^* \times \mathbb{Q}.$$

Si nos preguntamos qué es $g(0)$, tendremos problemas. Por un lado, $\frac{0}{|0|}$ no es ningún número. Por otro lado, 0 no es un elemento del dominio de g. Luego la expresión $g(0)$ no tiene referencia alguna, es decir, no representa ningún objeto. Lo mismo sucede con la función $r(x) =$ "el rey de x", que no incluye a $C =$ "Colombia" en su dominio, puesto que $r(C) =$ "el rey de Colombia" no se refiere a ninguna persona.

Si recordamos la definición de imagen de una relación, para cualquier función $f : A \to B$ tenemos que

$$\begin{aligned} \textsc{img}(f) &= \{y : \exists x \in \textsc{dom}(f) : (x, y) \in f\} \\ &= \{y : \exists x \in A : y = f(x)\} \\ &= \{f(x) : x \in A\}. \end{aligned}$$

Para la función f del ejemplo 4.35, sabemos que $\text{IMG}(f) \subseteq \mathbb{Z}^-$. Sin embargo, la igualdad *no* se da:

$$\text{IMG}(f) = \{f(0), f(1), f(2), \dots\} = \{-1, -2, -5, \dots\}.$$

Ejemplo 4.36 (Funciones dadas como tuplas). Sea $n \in \mathbb{N}$. Dados $A_n = \{1, 2, \dots, n\}$ y B un conjunto cualquiera, una función $f : A_n \to B$ puede representarse mediante la n-tupla $(f(1), f(2), \dots, f(n))$. Por ejemplo, la tupla $f = (3, 6, \dots, 3n)$ representa la función dada por $f(k) = 3k$, para $k = 1, 2, \dots, n$.

En general, la intersección de dos relaciones es una relación, pues si $R_1 \subseteq A_1^2$ y $R_2 \subseteq A_2^2$, entonces $R_1 \cap R_2 \subseteq A_1^2 \cap A_2^2 = (A_1 \cap A_2)^2$. Para el caso de las funciones sucede lo mismo, es decir, la intersección de dos funciones (y esta expresión tiene sentido, ya que una función es un *conjunto* de parejas ordenadas) es también una función.

Teorema 4.37. Si $f_1 : A_1 \to B_1$ y $f_2 : A_2 \to B_2$, entonces $f = f_1 \cap f_2$ es una función, $\text{DOM}(f) \subseteq A_1 \cap A_2$ e $\text{IMG}(f) \subseteq \text{IMG}(f_1) \cap \text{IMG}(f_2)$.

Prueba. Ya hemos notado que f es una relación. Si $x \in \text{DOM}(f)$, entonces existe y tal que $(x, y) \in f_1 \cap f_2$; esto implica, en consecuencia, que

$$x \in \text{DOM}(f_1) \cap \text{DOM}(f_2) = A_1 \cap A_2.$$

Asimismo podemos probar que $\text{IMG}(f) \subseteq \text{IMG}(f_1) \cap \text{IMG}(f_2)$. Demostremos que f es una función: si $(x, y), (x, y') \in f = f_1 \cap f_2$, entonces en particular, tenemos que $(x, y), (x, y') \in f_1$. Como f_1 es una función, concluimos que $y = y'$. ∎

Dadas dos funciones f_1 y f_2, diremos que f_2 es una *extensión* de f_1, f_2 *extiende* a f_1, o que f_1 es una *restricción* de f_2, si $f_1 \subseteq f_2$. *Extensión* *Restricción*

☞ **Antes de seguir leyendo**

Sean $f_1 : A_1 \to B_1$, $f_2 : A_2 \to B_2$. Para cada una de las siguientes afirmaciones determine si es verdadera en general:

1. Si f_1 es una restricción de f_2, entonces se tiene que $A_1 \subseteq A_2$ y que $\text{IMG}(f_1) \subseteq \text{IMG}(f_2)$.
2. Si $A_1 \subseteq A_2$ e $\text{IMG}(f_1) \subseteq \text{IMG}(f_2)$, entonces f_2 extiende a f_1.
3. $f_1 \cup f_2$ es una función.

Finalizamos esta sección con un listado de las distintas maneras de expresar el hecho de que $f(x) = y$, donde f es una función:

Observación 4.38. Sea $f : A \to B$ una función. Entonces las siguientes expresiones son equivalentes:

(a) $(x, y) \in f$;
(b) $x f y$;
(c) $f(x) = y$;
(d) $x \overset{f}{\mapsto} y$;
(e) y es la imagen de x (bajo f);
(f) x es una preimagen de y (bajo f).

Composición de funciones

$\circ$: *Composición de relaciones*

Definición 4.39 (Composición de relaciones). Si R y S son relaciones, definimos la relación $R \circ S := \{(a, c) : \text{existe } b \text{ tal que } (a, b) \in S \text{ y } (b, c) \in R\}$. Esta relación se lee "$R$ compuesto S".

En particular, dos funciones pueden componerse, dado que son relaciones. Consideremos el caso en que tenemos dos funciones $f : B \to C$ y $g : A \to B$. Por definición de composición:

$$\begin{aligned} f \circ g &= \{(x, z) : (x, y) \in g, (y, z) \in f, \text{ para algún } y \in B\} \\ &= \{(x, z) : g(x) = y, f(y) = z, \text{ para algún } y \in B\} \\ &= \{(x, z) : f(g(x)) = z\}. \end{aligned}$$

Note que $f \circ g$ es una función, pues si $(x, z), (x, z') \in f \circ g$, se tiene entonces que $z = f(g(x)) = z'$.

Por lo anterior, $f \circ g$ es el conjunto de parejas de la forma $(x, f(g(x)))$. Retomemos la analogía de las funciones vistas como máquinas: si f y g son máquinas, entonces $h = f \circ g$ es la máquina que *funciona* así:

1. h recibe un elemento x y lo introduce en la máquina g para obtener $c = g(x)$.
2. h introduce a c en la máquina f para obtener $f(c) = f(g(x))$.
3. En resumen, h ha transformado x en $h(x) = f(g(x))$.

En dicho proceso la máquina h le aplica primero g a x. Para que esto tenga sentido se requiere que $x \in \text{DOM}(g) = A$. Ahora, si $x \in \text{DOM}(g)$,

entonces tenemos que

$$c = g(x) \in \text{IMG}(g) \subseteq B = \text{DOM}(f).$$

Luego f puede aplicarse a c, y $h(x) = f(c)$ tiene sentido, esto es, h está bien definida. Además, $h(x) = f(g(x)) \in \text{IMG}(f) \subseteq C$. Concluimos que $\text{DOM}(f \circ g) = A$ y que $\text{IMG}(f \circ g) \subseteq C$, es decir,

$$f \circ g : A \to C.$$

$f \circ g$: Composición de funciones

Definición 4.40 (Composición de funciones). Sean $g : A \to B$ y $f : B \to C$ funciones. Entonces $f \circ g$ es la siguiente función:

$$\begin{aligned} f \circ g : A &\to C \\ x &\mapsto f(g(x)). \end{aligned}$$

Es decir, $(f \circ g)(x) = f(g(x))$.

Si f y g son como arriba y $h = f \circ g$, entonces decimos que $f \circ g$ es una *factorización* de h. Esto lo podemos expresar mediante cualquiera de los siguientes diagramas, diciendo además que éstos *conmutan*, es decir, que si le aplicamos g a un elemento cualquiera de A, y luego le aplicamos f, obtenemos el mismo resultado que si le aplicamos directamente la función h a tal elemento (véase la Figura 4.5).

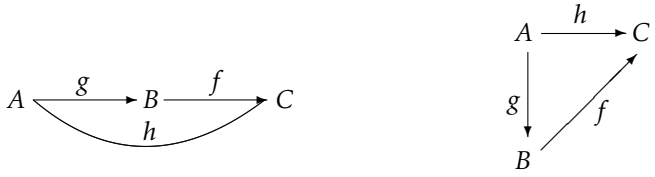


Figura 4.5 : Diagramas de composición de funciones. Ambos diagramas son equivalentes y expresan el hecho de que $h = f \circ g$.

Ejemplo 4.41. Sea $f : \mathbb{N} \to \mathbb{N}$ la función definida como $f(x) = 5x$ y sea $g : \mathbb{N} \to \mathbb{N}$ la función definida como $g(x) = x + 4$. Entonces $h = (f \circ g) : \mathbb{N} \to \mathbb{N}$ es la función definida como

$$h(x) = f(g(x)) = f(x + 4) = 5(x + 4) = 5x + 20.$$

Por otro lado, $h' = (g \circ f) : \mathbb{N} \to \mathbb{N}$ es la función definida como $h'(x) = g(f(x)) = g(5x) = 5x + 4$. Note que h y h' son funciones distintas. Por ejemplo, $h(1) = 25 \neq 9 = h'(1)$. Luego $(1, 25) \in h \setminus h'$.

Observación 4.42. La composición de funciones no es conmutativa.

☞ **Antes de seguir leyendo**

Demuestre que si $f : A \to B$, entonces

1. $f \circ \mathrm{ID}_A = f$; 2. $\mathrm{ID}_B \circ f = f$.

Finalmente observamos que la composición de funciones es *asociativa*. Esto es, si $f : A \to B$, $g : B \to C$ y $h : C \to D$, entonces:

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Esta igualdad es válida, pues ambas funciones tienen el mismo dominio A, y para todo elemento $a \in A$ tenemos:

$$\begin{aligned}((h \circ g) \circ f)(a) &= (h \circ g)(f(a)) \\ &= h(g(f(a))) \\ &= h((g \circ f)(a)) \\ &= (h \circ (g \circ f))(a).\end{aligned}$$

Funciones inyectivas, sobreyectivas y biyectivas

Definición 4.43 (Funciones inyectivas, sobreyectivas o biyectivas). Dada una función $f : A \to B$, diremos que:

Función inyectiva
(a) f es *inyectiva* (o *uno a uno*, 1:1, o f es una *inyección*) si y sólo si dados $x, y \in A$, $x \neq y$ implica $f(x) \neq f(y)$.

Función sobreyectiva
(b) $f : A \to B$ es *sobreyectiva* (o *sobre*, o f es una *sobreyección*) si y sólo si $\mathrm{IMG}(f) = B$.

Función biyectiva
(c) f es *biyectiva* (o f es una *biyección*) si f es inyectiva y sobreyectiva.

Así, una función f es inyectiva si envía elementos distintos a imágenes distintas, y $f : A \to B$ es sobreyectiva si para todo $y \in B$ existe $x \in A$ tal que $f(x) = y$.

☞ **Antes de seguir leyendo**

Sea P el conjunto de los policías y L el conjunto de los ladrones. Supongamos que cada policía x ha capturado exactamente a un ladrón y (posiblemente con ayuda de otros policías), de modo que existe una función "captura" $c : P \to L$ tal que $c(x)$ es igual a "el ladrón que fue capturado con ayuda del policía x". Bajo cada una de

las siguientes tres hipótesis, ¿cómo se comparan los tamaños de los conjuntos P y L? ¿Es alguno necesariamente menor o igual al otro?

1. Supongamos que c es una función inyectiva. Esto quiere decir que dos policías distintos capturan a ladrones distintos.
2. Supongamos que c es una función sobreyectiva. Esto quiere decir que para todo ladrón y existe por lo menos un policía x que lo captura (es decir, tal que $c(x) = y$).
3. Supongamos que c es una función biyectiva. Esto quiere decir que para todo ladrón y existe exactamente un policía x que lo captura, esto es, tal que $c(x) = y$.

☞ **Antes de seguir leyendo**

1. Demuestre que la función identidad $f : A \to A$ es una biyección.
2. Diremos que una función $f : A \to B$ es *constante* si $\text{IMG}(f)$ es un *singleton*. Encuentre una condición necesaria y suficiente para que una función constante $f : A \to B$ sea una biyección.
3. Demuestre que la función $\varnothing : \varnothing \to \varnothing$ es una biyección. (*Ayuda*: ¿qué ocurriría si no fuera 1:1? ¿Si no fuera sobreyectiva?)

Note que las propiedades de sobreyectividad y biyectividad no dependen exclusivamente de la función f, sino además del conjunto B. En ese orden de ideas, lo correcto sería afirmar que f es una función sobreyectiva *entre* A *y* B.

Decir que una función f es inyectiva es decir que f no puede enviar puntos distintos a imágenes iguales; en otras palabras, que la única forma de que ocurra que $f(x) = f(y)$ es que $x = y$.

Observación 4.44. Una función $f : A \to B$ es inyectiva si y sólo si dados $x, y \in A$, si $f(x) = f(y)$ entonces $x = y$.[2]

Esta observación permite nos demostrar la inyectividad de una función de la siguiente forma:

suponer que $f(x) = f(y)$ y, a partir de esta igualdad,
concluir que $x = y$.

[2] "Si $f(x) = f(y)$, entonces $x = y$" es la contrarrecíproca de la afirmación "si $x \neq y$, entonces $f(x) \neq f(y)$". En general, una proposición de la forma $p \to q$ y su contrarrecíproca $\neg q \to \neg p$ son lógicamente equivalentes.

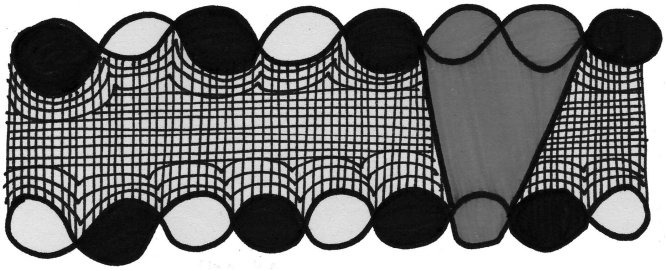


Figura 4.6: Una función es inyectiva si *no* envía elementos distintos a la misma imagen. La figura representa de forma esquemática una función que no es inyectiva.

Recordemos que una función $f : A \to B$ es sobreyectiva si y sólo si para todo $y \in B$ existe $x \in A$ tal que $f(x) = y$. Por eso, para demostrar que $f : A \to B$ es sobreyectiva se procederá normalmente así: sea $y \in B$; a partir de este elemento y se construye, o se halla, un elemento $x \in A$ apropiado para que se verifique $f(x) = y$.

En general, aunque una función dada $f : A \to B$ sea invertible, de ahí no se sigue que $\text{DOM}(f^{-1})$ sea igual a B. Esto ocurre sólo en el caso de que f sea sobreyectiva, ya que en general se tiene que $\text{DOM}(f^{-1}) = \text{IMG}(f)$.

Ejemplo 4.45. Sea $f : \mathbb{R} \to \mathbb{R}$ la función dada por $f(x) = 2x + 1$. Veamos que f es una biyección:

(a) Inyectividad: si $f(x) = f(y)$, entonces $2x + 1 = 2y + 1$. Por ende, $2x = 2y$ y $x = y$.

(b) Sobreyectividad: sea $y \in \mathbb{R}$. Debemos encontrar un elemento $x \in \text{DOM}(f) = \mathbb{R}$ tal que $f(x) = y$, esto es, $2x + 1 = y$. Tomamos $x = (y - 1)/2$. Se tiene que $x \in \mathbb{R}$ y, además, que

$$f(x) = f((y-1)/2) = 2((y-1)/2) + 1 = y - 1 + 1 = y,$$

como queríamos.

En general, puede demostrarse que toda función $f : \mathbb{R} \to \mathbb{R}$ de la forma $f(x) = ax + b$, con $a \neq 0$, es una biyección.

Ejemplo 4.46. Sea $g : \mathbb{R} \to [0, \infty)$ la función $g(x) = x^2$. Es fácil ver que $\text{IMG}(g) = [0, \infty)$, luego g es sobreyectiva. Sin embargo, g no es inyectiva: $g(-3) = g(3)$, pero $3 \neq -3$. Es decir, sabiendo únicamente quién es $g(x)$, no podemos sabemos con seguridad quién es x.

Definición 4.47 (Función invertible). Diremos que una función f es *invertible* si y sólo si la relación f^{-1} es también una función. *Función invertible*

Es fácil ver que para toda relación R vale que $\text{DOM}(R^{-1}) = \text{IMG}(R)$, e $\text{IMG}(R^{-1}) = \text{DOM}(R)$. Concluimos que si $f : A \to B$ es invertible, entonces su inversa será una función $f^{-1} : \text{IMG}(f) \to A$.

Ejemplo 4.48. Sea $f : \mathbb{Z} \to \mathbb{R}$ la función dada por $f(r) = 3r$. Entonces tenemos que $f = \{(r, 3r) : r \in \mathbb{Z}\}$, de modo que conjuntistamente

$$f^{-1} = \{(3r, r) : r \in \mathbb{Z}\}.$$

Si $(3r, r), (3s, s) \in f^{-1}$ y $3r = 3s$, entonces $r = s$. Esto demuestra que f^{-1} es una función. Luego f es invertible. Sea $B = \{3r : r \in \mathbb{Z}\}$. Es claro que $B = \text{IMG}(f) = \text{DOM}(f^{-1})$ y que $\text{IMG}(f^{-1}) = \text{DOM}(f) = \mathbb{Z}$. Además, para todo $x \in B$ se tiene que $f^{-1}(x) = \frac{x}{3}$.

Teorema 4.49. Dada una función $f : A \to B$, tenemos que f es inyectiva si y sólo f es invertible.

Prueba. Se deja al lector (ejercicio 10). ∎

Note que si f es invertible, entonces $(f^{-1})^{-1} = f$, luego f^{-1} es invertible y, además, inyectiva, por el teorema anterior.

☞ **Antes de seguir leyendo**

Demuestre que si $f : A \to B$ es una función invertible, entonces:

1. $f^{-1} \circ f = \text{ID}_A$;
2. $f \circ f^{-1} = \text{ID}_S$, donde $S = \text{DOM}(f^{-1}) = \text{IMG}(f)$.

Muchas funciones pueden expresarse como composición de varias funciones básicas. Para determinar la inyectividad de una función, en varios casos es suficiente estudiar la inyectividad de las funciones básicas que la componen. Lo mismo ocurre con la sobreyectividad.

Teorema 4.50. Para $f : A \to B$, $g : B \to C$, tenemos que

(a) si f y g son inyectivas, entonces $g \circ f$ es inyectiva;
(b) si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva;
(c) si f y g son biyectivas, entonces $g \circ f$ es biyectiva.

Prueba.

(a) Si $g(f(x)) = g(f(y))$, por inyectividad de g, $f(x) = f(y)$. Ahora, por inyectividad de f, $x = y$. Esto prueba que $g \circ f$ es inyectiva.

(b) Sea $c \in C$. Por sobreyectividad de g, existe $b \in B$ tal que $g(b) = c$. Por sobreyectividad de f, existe $a \in A$ tal que $f(a) = b$. Por ende, se tiene que $c = g(f(a)) = (g \circ f)(a)$ y esto prueba que $g \circ f$ es sobreyectiva.

(c) Se deduce fácilmente de (a) y (b). ∎

¿Valen los recíprocos de las propiedades anteriores? La respuesta es que no. Sin embargo, por lo menos podemos contar con lo siguiente:

Teorema 4.51. Para $f : A \to B$, $g : B \to C$, tenemos que

(a) si $g \circ f$ es inyectiva, entonces f es inyectiva;

(b) si $g \circ f$ es sobreyectiva, entonces g es sobreyectiva.

Prueba.

(a) Sean $x, y \in A$ tales que $f(x) = f(y)$. Entonces $g(f(x)) = g(f(y))$, lo cual equivale a que

$$(g \circ f)(x) = (g \circ f)(y).$$

Por inyectividad de $g \circ f$, concluimos que $x = y$.

(b) Sea $c \in C$. Como $g \circ f : A \to C$ es una función sobreyectiva, se tiene entonces que existe $a \in A$ tal que

$$c = (g \circ f)(a) = g(f(a)).$$

Sea $b = f(a)$. Entonces $b \in B$ y $g(b) = c$. ∎

Definición 4.52 (Inversa por derecha e inversa por izquierda de funciones). Dada una función $f : A \to B$,

Inversa por izquierda

(a) una *inversa por izquierda* de f es una función $g : B \to A$ que cumple que $g \circ f = \mathrm{ID}_A$; y

Inversa por derecha

(b) una *inversa por derecha* de f es una función $h : B \to A$ que cumple que $f \circ h = \mathrm{ID}_B$.

La existencia de una inversa por izquierda o por derecha caracteriza respectivamente la inyectividad o sobreyectividad de una función:

Teorema 4.53. Sea $f : X \to Y$. Tenemos que

(a) f es inyectiva si y sólo si f tiene una inversa por izquierda;

(b) f es sobreyectiva si y sólo si f tiene una inversa por derecha.

Prueba.

(a) Utilizamos el método de doble implicación:

(→) Supongamos que f es inyectiva. Si X fuera vacío, entonces f sería la función vacía, que es su propia inversa por izquierda. Supongamos entonces que X no es vacío. Sea $x_0 \in X$ un elemento cualquiera. Definimos la función $g : Y \to X$ así: dado $y \in Y$, si $y \in \text{IMG}(f)$, entonces sea $g(y)$ el único elemento x en X tal que $f(x) = y$ (se tendrá entonces que $g(f(x)) = x$); si $y \notin \text{IMG}(f)$, sea $g(y) = x_0$. Por construcción, tenemos que para todo $x \in X$, $g(f(x)) = x$ y de esta manera podemos concluir que $g \circ f = \text{ID}_X$.

(←) Supongamos que existe una función $g : Y \to X$ que cumple que $g \circ f = \text{ID}_X$. Veamos que f es inyectiva: sean $x_1, x_2 \in X$ tales que $f(x_1) = f(x_2)$. Así $g(f(x_1)) = g(f(x_2))$, luego $x_1 = x_2$.

(b) Utilizamos el método de doble implicación:

(→) Supongamos que f es sobreyectiva. Construimos la función $g : Y \to X$ de la siguiente forma: dado un elemento $y \in Y$, consideremos el conjunto $E_y = \{x \in X : f(x) = y\}$: este es el conjunto de las preimágenes de y bajo f. Como f es sobreyectiva, el conjunto E_y es no vacío. Luego podemos *elegir* algún elemento de este conjunto que llamaremos $g(y)$. Veamos que $f \circ g = \text{ID}_Y$: dado $y \in Y$, sabemos que $g(y) \in E_y$, por ende, $f(g(y)) = y$. Esto era lo que queríamos demostrar.

(←) Supongamos que existe $g : Y \to X$ tal que $f \circ g = \text{ID}_Y$ y veamos que $f : X \to Y$ es sobreyectiva: sea $y \in Y$. Entonces $f(g(y)) = y$, luego $g(y)$ es una preimagen de y bajo f. Esto demuestra que f es sobreyectiva. ∎

Corolario 4.54. Sea A un conjunto y sean f y g funciones tales que $g \circ f = \text{ID}_A$. Entonces f es inyectiva y g es sobreyectiva.

Teorema 4.55. Sean $f : A \to B$, $g : B \to A$ y $h : B \to A$, tales que g es una inversa por izquierda de f, y h es una inversa por derecha de f. Entonces $f^{-1} = g = h$.

Prueba. Supongamos que f tiene inversas $g : B \to A$ y $h : B \to A$, por izquierda y por derecha respectivamente. La existencia de h garantiza que B es la imagen de f y la existencia de g garantiza que f es invertible; luego f^{-1} es una función con dominio $\text{IMG}(f) = B$. Bajo las anteriores condiciones podemos concluir que g y h son la misma función.

Lo anterior se demuestra así: sabemos que $\text{ID}_A = g \circ f$, luego

$$\begin{aligned} f^{-1} &= \text{ID}_A \circ f^{-1} \\ &= (g \circ f) \circ f^{-1} \\ &= g \circ (f \circ f^{-1}) \\ &= g \circ \text{ID}_{\text{DOM}(f^{-1})} \\ &= g \circ \text{ID}_B = g. \end{aligned}$$

Así, $f^{-1} = g$. Ahora, $\text{ID}_B = f \circ h$, luego

$$\begin{aligned} f^{-1} &= f^{-1} \circ \text{ID}_B \\ &= f^{-1} \circ (f \circ h) \\ &= (f^{-1} \circ f) \circ h \\ &= \text{ID}_A \circ h \\ &= h. \end{aligned}$$

Concluimos que $f^{-1} = g = h$, como se quería. ∎

A continuación enunciamos un criterio útil para verificar si una función es biyectiva:

Teorema 4.56. Sean $f : A \to B$, $g : B \to A$ funciones. Si $g \circ f = \text{ID}_A$ y $f \circ g = \text{ID}_B$, entonces f y g son biyectivas y mutuamente inversas, esto es, $f^{-1} = g$ y $g^{-1} = f$.

Prueba. Como f tiene a g como inversa por izquierda y por derecha, entonces f es biyectiva por el Teorema 4.53. De manera análoga podemos concluir que g es una biyección. Por un método similar al empleado en la demostración del Teorema 4.55, podemos concluir que $f^{-1} = g$. Finalmente $f = (f^{-1})^{-1} = g^{-1}$. ∎

Lema 4.57. Consideremos dos funciones $f_0 : A_0 \to B_0$ y $f_1 : A_1 \to B_1$, donde $A_0 \cap A_1 = \varnothing$ y $B_0 \cap B_1 = \varnothing$. Sea $f : A_0 \cup A_1 \to B_0 \cup B_1$ la función definida así:

$$f(x) = \begin{cases} f_0(x) & \text{si } x \in A_0; \\ f_1(x) & \text{si } x \in A_1. \end{cases}$$

Entonces se tienen las siguientes propiedades:

(a) Si f_0 y f_1 son inyectivas, entonces f también lo es.

(b) $\text{IMG}(f) = \text{IMG}(f_0) \cup \text{IMG}(f_1)$. Por lo tanto, si f_0 y f_1 son sobreyectivas, entonces f también lo es.

Prueba. Verificamos (a) y dejamos la demostración de (b) al lector (ejercicio 11). Sean $x, y \in A_0 \cup A_1$ tales que $f(x) = f(y)$. Como $f(x) \in B_0 \cup B_1$, hay dos casos por considerar:

(i) $f(x) \in B_0$: entonces $x \in A_0$, pues de lo contrario se tendría $x \in A_1$ y consecuentemente $f(x) = f_1(x) \in B_1$, lo que no es posible pues B_0 y B_1 son disjuntos. Análogamente $y \in A_0$. Entonces tenemos que

$$f_0(x) = f(x) = f(y) = f_0(y).$$

Como f_0 es inyectiva, concluimos que $x = y$.

(ii) $f(x) \in B_1$: este caso es similar a (i).

Debido a que en cualquier caso obtenemos que $x = y$, podemos concluir que f es inyectiva. ∎

Imagen y preimagen de una función

A partir de las definiciones de imagen y preimagen de una relación, en particular, se tiene que si $f : A \to B$ es una función y $S \subseteq A$, $T \subseteq B$, entonces

(a) $f[S] = \{y : \exists x \in S : (x, y) \in f\}$
$= \{y : \exists x \in S : y = f(x)\}$
$= \{f(x) : x \in S\}.$

$f[S]$: Imagen de f bajo S

(b) $f^{-1}[T] = \{x \in A : \exists y \in T : (x, y) \in f\}$
$= \{x \in A : f(x) \in T\}.$

$f^{-1}[T]$: Preimagen de f bajo T

Para fines prácticos, los dos hechos más importantes de los conjuntos $f[S]$ y $f^{-1}[T]$ son los siguientes:

(i) Si $x \in S$, entonces $f(x) \in f[S]$ (aunque no necesariamente vale la recíproca).

(ii) $f(x) \in T$ si y sólo si $x \in f^{-1}[T]$.

Definición 4.58 (fibra). Dada una función $f : A \to B$ y $b \in B$, llamaremos la *fibra sobre b con respecto a f* al conjunto

Fibra

$$f^{-1}[\{b\}] = \{a \in A : f(a) = b\}.$$

En otras palabras, la fibra sobre b con respecto a f es el conjunto de todas la preimágenes de b con respecto a f.

Recordemos que una función $f : A \to B$ es sobreyectiva si y sólo si para todo $b \in B$ existe $a \in A$ tal que $f(a) = b$. En otras palabras, si para todo $b \in B$, la fibra sobre b es un conjunto no vacío. Este hecho se utilizó en la demostración del Teorema 4.53 (b).

Por definición una función $f : A \to B$ *no* es inyectiva si existen x y y tales que $x \neq y$ y $f(x) = f(y)$. En este caso tanto x como y pertenecen a la fibra de $f(x)$ y, por ende, esta fibra tiene más de un elemento.

Podemos resumir estas afirmaciones de la siguiente forma:

Observación 4.59. Dada una función $f : A \to B$:

(a) f es inyectiva si y sólo si para todo $b \in B$, la fibra $f^{-1}[\{b\}]$ tiene a lo sumo un elemento;

(b) f es sobreyectiva si y sólo si para todo $b \in B$, la fibra $f^{-1}[\{b\}]$ tiene al menos un elemento;

(c) f es biyectiva si y sólo si para todo $b \in B$, la fibra $f^{-1}[\{b\}]$ es un *singleton*.

Ejemplo 4.60. Sean $A = \{1,2,3,4,5,6\}$, $B = \{a,b,c,d,e\}$ y $f : A \to B$ la función dada por la tupla (c,e,a,d,b,e), esto es, $f(1) = c, f(2) = e$, $f(3) = a$, etc.). Entonces, por ejemplo:

(a) $f[A] = B$;
(b) $f[\{1,2,3\}] = \{a,c,e\}$;
(c) $f[\{2,6\}] = \{e\}$;
(d) $f^{-1}[B] = A$;
(e) $f^{-1}[\{a,e\}] = \{2,3,6\}$;
(f) $f^{-1}[f[\{2\}]] = \{2,6\}$.

☞ **Antes de seguir leyendo**

Sea $f : X \to Y$. Demuestre las siguientes afirmaciones:

1. $f[\varnothing] = f^{-1}[\varnothing] = \varnothing$.
2. Si $x \in X$, entonces $f(\{x\}) = \{f(x)\}$.

A continuación estudiaremos las propiedades de $f[X]$ y $f^{-1}[Y]$:

Teorema 4.61. Para $f : A \to B$, $X, X' \subseteq A$, tenemos:

(a) *monotonía*: $X \subseteq X'$ implica $f[X] \subseteq f[X']$;
(b) $f[X \cup X'] = f[X] \cup f[X']$;
(c) $f[X \cap X'] \subseteq f[X] \cap f[X']$.

Prueba.

(a) Supongamos que $X \subseteq X'$ y verifiquemos que $f[X] \subseteq f[X']$: si es el caso que $y \in f[X]$, entonces existe $x \in X$ tal que $y = f(x)$. Por hipótesis, $x \in X'$. En consecuencia, por definición, $f(x) \in f[X']$, es decir, $y \in f[X']$.

(b) Utilizamos el método de doble inclusión:

(⊆) Si $y \in f[X \cup X']$, entonces $y = f(a)$ para cierto $a \in X \cup X'$. Si $a \in X$, entonces $y \in f[X]$. Si $a \in X'$, entonces $y \in f[X']$. Por ende, $y \in f[X] \cup f[X']$.

(⊇) Como $X, X' \subseteq X \cup X'$, por la parte (a) tenemos entonces que $f[X] \subseteq f[X \cup X']$ y $f[X'] \subseteq f[X \cup X']$, lo que implica que

$$f[X] \cup f[X'] \subseteq f[X \cup X'].$$

(c) Como $X \cap X' \subseteq X$ y $X \cap X' \subseteq X'$, por la parte (a) tenemos que $f[X \cap X'] \subseteq f[X]$ y $f[X \cap X'] \subseteq f[X']$, lo que implica que

$$f[X \cap X'] \subseteq f[X] \cap f[X'].$$ ∎

Como lo muestra el siguiente teorema, la operación de preimagen $f^{-1}[\,]$ se comporta *mejor* que la operación de imagen $f[\,]$, pues $f^{-1}[\,]$ preserva además, la intersección:

Teorema 4.62. Para $f : A \to B$, $Y, Y' \subseteq B$, tenemos:

(a) *monotonía*: $Y \subseteq Y'$ implica $f^{-1}[Y] \subseteq f^{-1}[Y']$.

(b) $f^{-1}[Y \cup Y'] = f^{-1}[Y] \cup f^{-1}[Y']$.

(c) $f^{-1}[Y \cap Y'] = f^{-1}[Y] \cap f^{-1}[Y']$.

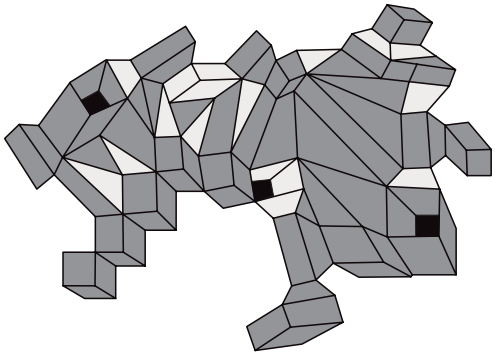
Prueba. Demostramos (b) por el método directo y dejamos (a) y (c) al lector (ejercicio 12).

Dado un x cualquiera, tenemos:

$$\begin{aligned} x \in f^{-1}[Y \cup Y'] &\leftrightarrow f(x) \in Y \cup Y' && \text{(df. } f^{-1}\text{)} \\ &\leftrightarrow f(x) \in Y \vee f(x) \in Y' && \text{(df. unión)} \\ &\leftrightarrow x \in f^{-1}[Y] \vee x \in f^{-1}[Y'] && \text{(df. } f^{-1}\text{)} \\ &\leftrightarrow x \in f^{-1}[Y] \cup f^{-1}[Y']. && \text{(df. unión)} \end{aligned}$$

∎

Ejercicios



1. Sea $f : \mathbb{R} \to \mathbb{R}$ la función dada por $f(x) = 6 - x$.
   (a) Calcule $f(3)$ y $f(f(5))$.
   (b) Demuestre que f es una biyección.
2. Sea $f : \mathbb{Q} \to \mathbb{Q}$ la función dada por $f(x) = 2|x| - 1$. ¿Qué conjunto es $\text{IMG}(f)$? ¿Es f 1-1? ¿Es f sobreyectiva?
3. Provea un ejemplo de las siguientes:
   (a) Dos funciones f y g cuya composición $f \circ g$ sea inyectiva, pero alguna de ellas no lo sea.
   (b) Dos funciones f y g cuya composición $f \circ g$ sea sobreyectiva, pero alguna de ellas no lo sea.
4. Dé un ejemplo de una función $f : A \to A$ que sea inyectiva y no sea sobreyectiva.
5. Dados $f : A \to A$ y $S \subseteq A$, definimos recursivamente f^n de la siguiente manera: $f^0 = \text{ID}_A$, $f^{n+1} = f \circ f^n$. Dado $A = \{1, 2, 3, 4, 5\}$, encuentre una función $f : A \to A$, tal que 4 sea el mínimo número natural n tal que $f^n(A) = \{3\}$.
6. Sean $f : A \to B$, $X \subseteq A$ y $Y \subseteq B$.
   (a) Demuestre que $X \subseteq f^{-1}[f[X]]$ (¿bajo qué condición sobre f vale siempre la igualdad?).
   (b) Demuestre que $f[f^{-1}[Y]] \subseteq Y$ (¿bajo qué condición sobre f vale siempre la igualdad?).
   (c) Concluya lo siguiente:

$$f[f^{-1}[f[X]]] = f[X];$$
$$f^{-1}[f[f^{-1}[Y]]] = f^{-1}[Y].$$

7. Para $i = 1, \dots, n$, sea $f_i : A_i \to A_{i+1}$ una biyección. Demuestre que
$$(f_n \circ f_{n-1} \circ \cdots \circ f_1)^{-1} = f_1^{-1} \circ f_2^{-1} \circ \cdots \circ f_n^{-1}.$$
8. Sea $f : A \to B$. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:
   (a) Para $X, X' \subseteq A$, si X y X' son disjuntos entonces $f[X]$ y $f[X']$ son disjuntos.
   (b) Para $Y, Y' \subseteq B$, si Y y Y' son disjuntos entonces $f^{-1}[Y]$ y $f^{-1}[Y']$ son disjuntos.
   (c) Para $x \in A$, si $f(x) \in f[X]$, entonces $x \in X$.
   (d) Para $x \in A$, $f^{-1}[\{f(x)\}] = \{x\}$.
9. Sean $A, B \subseteq \mathbb{R}$ y sea $f : A \to B$. Supongamos que f es *estrictamente creciente*, es decir, dados $a, a' \in A$, si $a < a'$ entonces $f(a) < f(a')$. Demuestre que f es inyectiva.
10. Demuestre el Teorema 4.49.
11. Demuestre la parte (b) del Lema 4.57.
12. Demuestre las partes (a) y (c) del Teorema 4.62.
13. Sean A, B conjuntos disjuntos y sea $f : A \times B \to \mathcal{P}(A \cup B)$ la función dada por $f((a,b)) = \{a, b\}$. Demuestre que f es inyectiva.
14. Sea $f : \mathcal{P}(\mathbb{Z}) \to \mathcal{P}(\mathbb{Z})$ la función dada por $f(A) = A \cap \mathbb{N}$.
   (a) Calcule $f(\mathbb{Z})$, $f(\{-2, 1, 0, 1, 2, 3\})$ y $f(\varnothing)$.
   (b) Demuestre que f es sobreyectiva pero no es biyectiva.
15. Sea $B = \{2, -1, -4, -7, -10, -13 \dots\}$. Defina una función biyectiva $f : \mathbb{Z} \to B$ y demuestre que es biyectiva.
16. Sea $f : \mathcal{P}(\mathbb{Z}) \to \mathcal{P}(\mathbb{Z})$ la función definida así:
$$f(S) = \{z + 1 : z \in S\} \qquad (S \in \mathcal{P}(\mathbb{Z})).$$
Demuestre que f es biyectiva.
17. Sea $f : X \to Y$ una función cualquiera, y sean φ, ψ las funciones *imagen* y *preimagen*, respectivamente. Esto es,
$$\varphi : \mathcal{P}(X) \to \mathcal{P}(Y), \quad \varphi(S) = f[S] = \{f(s) \in Y : s \in S\};$$
$$\psi : \mathcal{P}(Y) \to \mathcal{P}(X), \quad \psi(T) = f^{-1}[T] = \{x \in X : f(x) \in T\}.$$
   (a) Demuestre que las siguientes afirmaciones son equivalentes:
      (i) f es inyectiva;
      (ii) φ es inyectiva;
      (iii) ψ es sobreyectiva.

(b) Demuestre que las siguientes afirmaciones son equivalentes:

(i) f es sobreyectiva;

(ii) φ es sobreyectiva;

(iii) ψ es inyectiva.

(c) Demuestre que f es una biyección si y sólo si φ y ψ son funciones mutuamente inversas.

18. Para cada número natural n, sea f_n una función cualquiera.

(a) Demuestre que $f = \bigcap_{n\in\mathbb{N}} f_n$ es también una función. (Recuerde que f_n es el conjunto $\{(x, f_n(x)) : x \in \operatorname{DOM}(f_n)\}$).

(b) ¿Cómo se comparan los conjuntos $\operatorname{DOM}(f)$ y $\bigcap_{n\in\mathbb{N}} \operatorname{DOM}(f_n)$?

(c) ¿Cómo se comparan los conjuntos $\operatorname{IMG}(f)$ y $\bigcap_{n\in\mathbb{N}} \operatorname{IMG}(f_n)$?

19. Defina una biyección explícita entre $\mathcal{P}(\{0,1,2,3\})$ y $\mathcal{P}(\{4,5,6,7\})$, y demuestre que en efecto esta función es biyectiva.

20. Sea $Q = \{S \subseteq \mathbb{N} : 0 \in S\}$. Defina una biyección explícita entre Q y $\mathcal{P}(\mathbb{N})$ y demuestre que en efecto esta función es biyectiva.

21. Sea X un conjunto no vacío. Demuestre que existe una biyección $f : \mathcal{P}(X) \to \mathcal{P}(X)$ que *no fija puntos*, esto es, que verifica $f(S) \neq S$, para cualquier $S \in \mathcal{P}(X)$.

Para los siguientes ejercicios considere esta definición:

Definición. Dados los conjuntos A y B, definimos A^B como el conjunto de todas las funciones $f : B \to A$.

22. Pensemos en el número 2 como el conjunto $\{0,1\}$ y sea X un conjunto cualquiera. Dado $A \in \mathcal{P}(X)$, sea $\chi_A : X \to 2$ la siguiente función:

$$\chi_A(x) = \begin{cases} 0 & \text{si } x \notin A; \\ 1 & \text{si } x \in A. \end{cases}$$

Note que esto define una función

$$\begin{aligned} \chi : \mathcal{P}(X) &\to 2^X \\ A &\mapsto \chi_A. \end{aligned}$$

Demuestre que χ es una biyección. (χ_A es llamada la *función característica de* A).

23. Dado $A \subseteq B$, definimos la función $f_A : \mathcal{P}(B) \to \mathcal{P}(B)$ como

$$f(X) = A \triangle X \qquad (X \in \mathcal{P}(B)).$$

(a) Demuestre que f_A es una función biyectiva.

(b) Demuestre que la función $\varphi : \mathcal{P}(B) \to B^B$ dada por $\varphi(A) = f_A$ es inyectiva, pero no es sobreyectiva si B tiene más de un elemento.

24. Dados los conjuntos S y X, con $S \subseteq X$, definimos la función

$$\varphi_{S\to X} : X^S \to X^X$$

así: dada $f \in X^S$, $\varphi_{S\to X}(f) : X \to X$ es la función dada por

$$\varphi_{S\to X}(f)(x) = \begin{cases} f(x) & \text{si } x \in S; \\ x & \text{si } x \in X \setminus S. \end{cases}$$

Demuestre las siguientes afirmaciones:

(a) Dada $f \in X^S$, $\text{IMG}_f = S$ si y sólo si $\varphi_{S\to X}(f) : X \to$ es sobreyectiva.

(b) $\varphi_{S\to X}$ es una función inyectiva.

(c) $\varphi_{S\to X}$ es una función sobreyectiva si y sólo si $S = X$.

(d) Si $S \subseteq T \subseteq X$, entonces $\varphi_{T\to X} \circ \varphi_{S\to T} = \varphi_{S\to X}$.

§ 4.4 Relaciones de equivalencia

Sea M un conjunto no vacío de mangos y B un conjunto no vacío de barriles distintos, tales que cada mango está en algún barril de B y todo barril de B es un conjunto no vacío de mangos de M. Es claro que si a, b y c son mangos de M tenemos que

(i) a y a se encuentran en el mismo barril;

(ii) si a se encuentra en el mismo barril que b, entonces necesariamente b se encuentra en el mismo barril que a;

(iii) si a se encuentra en el mismo barril que b y b se encuentra en el mismo barril que c, entonces necesariamente a se encuentra en el mismo barril que c.

En terminología matemática, definimos la relación $\sim$ sobre el conjunto M de la siguiente manera:

$a \sim b$ si y sólo si a se encuentra en el mismo barril que b.

Entonces la relación $\sim$ es reflexiva, simétrica y transitiva. Dado un mango $a \in M$ sea $[a]$ el único barril al cual pertenece. Sea $B = \{[a] : a \in M\}$ el conjunto de todos los barriles. A este conjunto lo podemos denotar así: $M/\sim$, y la justificación de esta notación es que hemos partido, repartido o dividido a M por medio de la relación $\sim$. Los mangos "pierden sus diferencias" dentro de cada barril y se vuelven *equivalentes*. Además,

hemos definido de forma sutil una función $f : M \to B$ dada por $f(a) = [a]$, que le asigna a cada mango el barril al cual pertenece.

La anterior relación es tan solo un ejemplo de la noción general de una *relación de equivalencia*, concepto que definimos a continuación:

Relación de equivalencia

Definición 4.63. Dado un conjunto X, una *relación de equivalencia* sobre X es una relación $E \subseteq X^2$ que es reflexiva, simétrica y transitiva.

Ejemplo 4.64 (Relaciones de equivalencia).

(a) Para un conjunto cualquiera X, $E = \text{ID}_X$ es una relación de equivalencia. Para demostrar esto, debemos verificar que E es reflexiva, simétrica y transitiva. (i) Para cualquier $x \in X$, $x = x$, es decir, xEx. Así, todo elemento de X se relaciona consigo mismo bajo E. (ii) Sean $x, y \in X$. Si xEy, entonces $x = y$. Luego $y = x$, esto es, yEx. (iii) Sean $x, y, z \in X$. Supongamos que xEy y yEz: entonces $x = y$ y $y = z$, luego $x = z$, esto es, xEz. En este ejemplo, los "barriles" de nuestra introducción a esta sección corresponden a conjuntos de un solo elemento, ya que bajo E todo $x \in X$ se relaciona únicamente consigo mismo.

(b) Sea $X = \mathbb{Z}$ y definamos la relación E sobre X así: aEb si y sólo si $a \equiv_2 b$, es decir, $\text{RES}_2(a) = \text{RES}_2(b)$ o, lo que es equivalente, $2 \mid a - b$. En virtud del Teorema 3.40, E es una relación de equivalencia.

En los anteriores ejemplos hemos utilizado de manera informal la noción de "barril" para designar algún conjunto de elementos relacionados entre sí según la relación de equivalencia. En adelante cambiaremos la palabra "barril" por la expresión "clase de equivalencia", pero el significado será esencialmente el mismo.

$[a]_E$: *Clase de equivalencia*

Definición 4.65 (Clase de equivalencia). Sea E una relación de equivalencia sobre un conjunto X. Dado $a \in X$, definimos *la clase de equivalencia de a con respecto a E*, y la denotamos $[a]_E$, así:

$$[a]_E := \{b \in X : aEb\}.$$

X/E: *Conjunto cociente*

Al conjunto de todas las clases de equivalencia lo simbolizamos X/E y se lo denomina *X partido por E* o *conjunto cociente de x con respecto a E*; esto es,

$$X/E := \{[a]_E : a \in X\}.$$

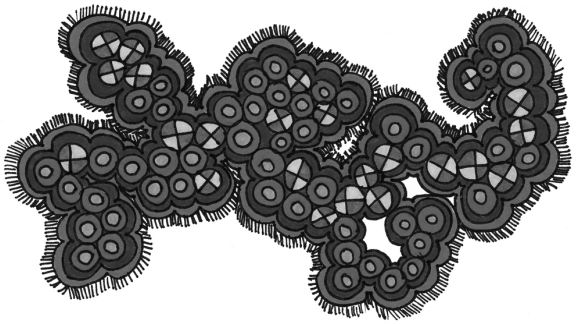


Figura 4.7 : Una clase de equivalencia representa un conjunto que ahora juega el papel de elemento. En otras palabras, todos los elementos de una clase de equivalencia se "unen" para formar un único elemento.

Por brevedad, llamaremos simplemente *clases* a las clases de equivalencia y denotaremos $[a]_E$ como $[a]$, cuando la relación E sea clara dentro del contexto. En algunas ocasiones debemos trabajar simultáneamente con varias relaciones de equivalencia $E, F, \ldots$ sobre un mismo conjunto X. En tal situación no podemos darnos el lujo de utilizar simplemente la expresión "$[a]$", pues ella podrá referirse a $[a]_E$ o $[a]_F$, que pueden ser conjuntos distintos.

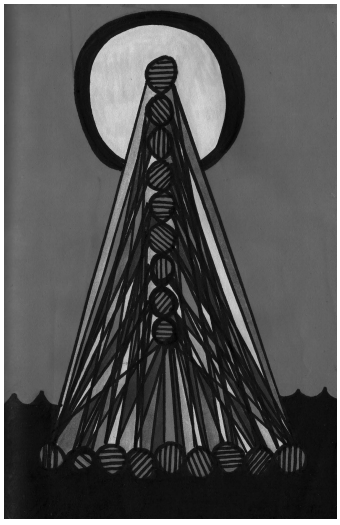


Figura 4.8 : Las relaciones de equivalencia "colapsan puntos".

A continuación estudiamos las clases de equivalencia generadas por las relaciones de los ejemplos anteriores.

Ejemplo 4.66.

(a) Si $E = \text{ID}_X$ y $a \in X$, entonces $[a] = \{b \in X : b = a\} = \{a\}$. Luego la clase de cualquier elemento es un *singleton*. En consecuencia, $X/E = \{\{a\} : a \in X\}$.

(b) Si $E = \equiv_2$ y $a \in \mathbb{Z}$, entonces se tiene que $[a] = \{b \in \mathbb{Z} : a - b \text{ es par}\} = \{\ldots, a-4, a-2, a, a+2, a+4, \ldots\}$. De esto concluimos lo siguiente:

(i) Si a es par, entonces $[a]$ es el conjunto de los pares.

(ii) Si a es impar, entonces $[a]$ es el conjunto de los impares.

Por lo tanto, si bien existe un número infinito de números enteros, sólo hay dos clases de equivalencia: $[0]$ y $[1]$. En este caso, $\mathbb{Z}/E = \{[0],[1]\} = \mathbb{Z}_2$. La relación E parte a $\mathbb{Z}$ en dos conjuntos *disjuntos y no vacíos*: los pares y los impares.

El siguiente ejemplo es de suma importancia y constituye un instrumento frecuente para construir relaciones de equivalencia:

Ejemplo 4.67 (Relación de equivalencia asociada a una función). Sea $f : X \to Y$ una función cualquiera. Definimos la relación E_f sobre X así: aE_fb si y sólo si $f(a) = f(b)$. Claramente E_f es una relación de equivalencia. Las clases corresponden precisamente a las fibras no vacías de f, esto es, a conjuntos de la forma $f^{-1}[\{y\}]$, con $y \in \text{IMG}(f)$. Para ver esto, notamos que

$$[a] = \{b \in X : f(b) = f(a)\} = f^{-1}[\{f(a)\}].$$

Si f es inyectiva, entonces toda clase es un *singleton* y, recíprocamente, si toda clase es un *singleton*, entonces f es inyectiva.

R_f: Relación de equivalencia asociada a f

La relación de equivalencia E_f introducida en el ejemplo anterior se denomina la *relación de equivalencia asociada a f*. Note que las relaciones dadas en (a) y (b) en el ejemplo 4.64 son *casos particulares* de E_f Para (a), tómese f la función identidad en A. Para (b), tómese $f : \mathbb{Z} \to \{0,1\}$, $f(x) = \text{RES}_2(x)$. Más adelante demostraremos que *toda* relación de equivalencia es de la forma E_f.

Definición 4.68. Sea E una relación de equivalencia sobre X y sea $a \in X$. Diremos que $b \in X$ es un *representante* de la clase $[a]$, si $b \in [a]$ o, de forma equivalente, si aEb. *Representante*

Teorema 4.69. Sea E una relación de equivalencia sobre X y $a, b \in X$. Tenemos entonces que

(a) a es un representante de $[a]$;
(b) $[a] = [b]$ si y sólo si aEb;
(c) $[a] \cap [b] \neq \varnothing$ si y sólo si aEb;
(d) $[a] \cap [b] = \varnothing$ si y sólo si a y b no se encuentran E-relacionados;
(e) $[a] \neq [b]$ si y sólo si $[a] \cap [b] = \varnothing$.

Prueba.

(a) Por reflexividad de E, tenemos que aEa. Luego $a \in [a]$.
(b) Si $[a] = [b]$, entonces $b \in [b] = [a]$, luego aEb. Para el recíproco, supongamos que aEb. Por simetría, bEa. Ahora, si $c \in [a]$, entonces aEc, luego por transitividad bEc, es decir, $c \in [b]$. Esto demuestra que $[a] \subseteq [b]$. Análogamente podemos probar que $[b] \subseteq [a]$. Luego $[a] = [b]$.
(c) Supongamos que $[a] \cap [b] \neq \varnothing$ y sea $c \in [a] \cap [b]$. Entonces aEc y bEc. Por simetría y transitividad, concluimos que aEb. Para el recíproco, si aEb, entonces $b \in [a]$, luego $b \in [a] \cap [b] \neq \varnothing$.
(d) Es una reformulación de la afirmación (c).
(e) Se deduce de las anteriores afirmaciones. ∎

Particiones

Finalizamos esta sección con un análisis de la noción de *partición*, la cual permite entender mejor las relaciones de equivalencia.

Definición 4.70 (Partición). Sea X un conjunto. Diremos que $P \subseteq \mathcal{P}(X)$ es una *partición* de X si y sólo si *Partición*

(a) $\varnothing \notin P$;
(b) $\bigcup P = X$;
(c) los conjuntos de P son disjuntos 2 a 2, es decir, si $S_1, S_2 \in P$ y $S_1 \neq S_2$, entonces $S_1 \cap S_2 = \varnothing$.

Si P es una partición de X, entonces por (b) y (c) tenemos que, para todo x, $x \in X$ si y sólo si existe un único $S \in P$ tal que $x \in S$.

☞ **Antes de seguir leyendo**

Demuestre que las siguientes afirmaciones son equivalentes:

(i) P es una partición de X;

(ii) $P \subseteq \mathcal{P}(X) \setminus \{\varnothing\}$ y para todo x, $x \in X$ si y sólo si existe un único $S \in P$ tal que $x \in S$.

En particular, todo elemento de X se encuentra en uno y sólo un elemento $S \in P$, de modo que P fragmenta a X en conjuntos disjuntos. Por ejemplo, el conjunto de barriles propuesto al comienzo de la sección es una partición del conjunto de mangos. Otro ejemplo de una partición consiste en la división política de un país X, visto como un conjunto de personas. En este caso, se parte X en regiones no vacías $S \in \mathcal{P}(X)$, disjuntas entre sí.

Ejemplo 4.71. Sea $X = \{1,2,3,4,5,6,7,8,9\}$. Entonces

$$P = \{\{1,9\},\{2,8\},\{3,4,5,6,7\}\}$$

es una partición de X en tres conjuntos:

$$\{1,9\},\{2,8\} \text{ y } \{3,4,5,6,7\}.$$

Note, por cierto, que $Q = \{\{1,2,9\},\{2,8\},\{3,4,5,6,7\}\}$ no es una partición de X.

El lector habrá notado que cada relación de equivalencia determina de manera natural una partición.

Teorema 4.72. Sea X un conjunto y $\sim$ una relación de equivalencia sobre X. Entonces $X/\sim$ es una partición de X.

Prueba. Sea $P = X/\sim$. Veamos que P es una partición de X:

(a) $\varnothing \notin P$: esto se tiene, pues si $a \in X$, entonces $a \in [a]$ y así $[a]$ no puede ser igual al conjunto vacío.

(b) $\bigcup P = X$: si $a \in \bigcup P$, entonces existe $S \in P$ tal que $a \in S$ y, como $S \subseteq X$, esto implica que $a \in X$. Para la otra inclusión, si $a \in X$, entonces $a \in [a] \in P$, luego $a \in \bigcup P$.

(c) Los elementos de P son disjuntos 2 a 2: si $[a],[b] \in P$ y $[a] \neq [b]$, entonces $[a]$ y $[b]$ son disjuntos (Teorema 4.69). ∎

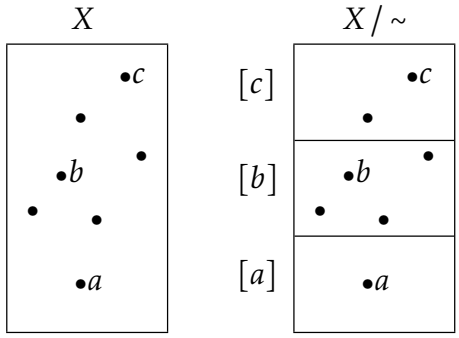


Figura 4.9: Si ~ es una relación de equivalencia sobre un conjunto X, entonces $X/\sim$ es una partición de X. Aquí X es un conjunto de siete elementos, mientras que la partición $X/\sim = \{[a],[b],[c]\}$ tiene tan sólo tres elementos.

La moraleja es la siguiente: toda relación de equivalencia sobre X automáticamente "induce" una partición sobre X. Como veremos a continuación, el fenómeno inverso ocurre también: *toda partición genera de manera natural una relación de equivalencia*.

Teorema 4.73. Dada una partición P de X, definamos la relación E_P sobre el conjunto X así:

$$aE_Pb \text{ si y sólo si existe } S \in P \text{ tal que } a,b \in S.$$

Entonces E_P es una relación de equivalencia.

Prueba. Sea $\sim = E_P$. Verifiquemos que ~ es una relación reflexiva, simétrica y transitiva:

(a) *Reflexividad*: sea $a \in X$. Como $\bigcup P = X$, existe $S \in P$ tal que $a \in S$. Entonces $a,a \in S$, luego $a \sim a$.

(b) *Simetría*: sean $a,b \in X$. Si $a \sim b$, existe $S \in P$ tal que $a,b \in S$, que es lo mismo que decir que $b,a \in S$, y esto prueba que $b \sim a$.

(c) *Transitividad*: sean $a,b,c \in X$. Supongamos que $a \sim b$ y $b \sim c$, y sean $S,T \in P$ tales que $a,b \in S$ y $b,c \in T$. Como P es una partición y $S \cap T \neq \varnothing$, entonces $S = T$, de modo que $a,c \in S$, y esto demuestra que $a \sim c$. ∎

Una demostración alternativa del teorema anterior es la siguiente: la definición de una partición P sobre X define de forma implícita una función $nat_P : X \to P$, dada por $nat_P(x) = P_x$, en donde P_x es el único elemento en P tal que $x \in P_x$. Ahora, si E_P es la relación definida en el Teorema 4.73, entonces claramente tenemos que aE_Pb si y sólo si $P_a = P_b$,

esto es, $nat_P(a) = nat_P(b)$. Por ende, E_P es la relación de equivalencia asociada a la función nat_P (véase el ejemplo 4.67).

Los teoremas anteriores permiten concebir las particiones como relaciones de equivalencia, y viceversa, por medio de las "operaciones" E_P y $X/\sim$, las cuales son mutuamente inversas:

Teorema 4.74. Para un conjunto X, una partición P de X y una relación de equivalencia $\sim$ sobre X,

$$\text{(a) } X/E_P = P; \qquad \text{(b) } E_{X/\sim} = \sim .$$

Prueba.

(a) Utilizamos el método de doble inclusión:

(⊆) Sea $[a]_{E_P} = [a] \in X/E_P$ y sea $S \in P$ tal que $a \in S$. Veamos que $[a] = S$: si $b \in [a]$, entonces aE_Pb, luego $a, b \in T$ para algún $T \in P$. Entonces $S \cap T \neq \varnothing$. Luego $S = T$ y así $b \in S$. Para la otra inclusión, si $b \in S$, entonces $a, b \in S$, luego aE_Pb, es decir, $b \in [a]$.

(⊇) Sea $S \in P$. Tome cualquier $a \in S$, el cual existe pues $S \neq \varnothing$. Es fácil verificar que $S = [a]_{E_P}$, luego $S \in X/E_P$.

(b) Utilizamos el método directo, es decir, demostramos que, para todo $x, y \in X$, se tiene que $(x, y) \in E_{X/\sim}$ si y sólo si $(x, y) \in \sim$:

$$\begin{aligned}(x,y) \in E_{X/\sim} &\leftrightarrow \exists S \in X/\sim : x, y \in S \\ &\leftrightarrow \exists a \in X : x, y \in [a]_\sim \\ &\leftrightarrow \exists a \in X : x \sim a \text{ y } y \sim a \\ &\leftrightarrow x \sim y.\end{aligned}$$

La justificación de la última equivalencia es la siguiente: (→) vale por simetría y transitividad. Para (←), tome $a = x$ (o $a = y$). ∎

☞ **Antes de seguir leyendo**

Demuestre que para toda relación de equivalencia E sobre X existe una función f tal que $E = E_f$.

Introducimos ahora la noción de *conjunto de representantes de una partición*. Intuitivamente, un conjunto C de representantes de una partición P de un conjunto X se construye eligiendo *exactamente* un elemento de cada clase $S \in P$. Bajo estas condiciones se tiene entonces que C es un subconjunto de X y que toda clase $S \in P$ interseca a C en *exactamente* un elemento.

Definición 4.75 (Conjunto de representantes). Sea P una partición de X. C es un *conjunto de representantes* de P si y sólo si $C \subseteq X$ y, para todo $S \in P$, existe $a \in X$ tal que $S \cap C = \{a\}$.

Conjunto de representantes

Ejemplo 4.76. Sea $X = \{0,1,2,3,4,5,6,7\}$ y sea P la siguiente partición sobre X:

$$P = \{\{0,1,2\},\{3,4\},\{5,6\},\{7\}\}.$$

Entonces es fácil verificar que $C = \{0,4,5,7\}$ es un conjunto de representantes de P, ya que todo elemento de la partición interseca a C en "exactamente un elemento". Intuitivamente, todo elemento $S \in P$ se encuentra representado por un único elemento $c \in C$ tal que $c \in S$. El lector puede convencerse de que la partición P admite exactamente doce conjuntos de representantes.

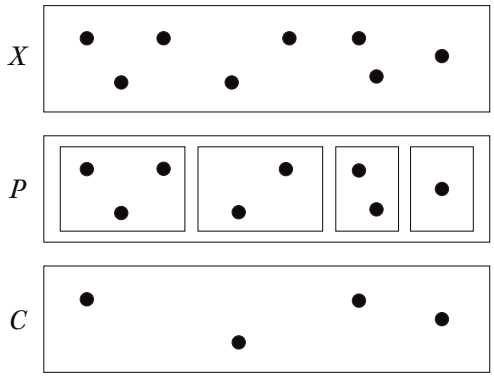


Figura 4.10: C es un conjunto de representantes de P (ejemplo 4.76).

La definición anterior puede darse también desde la perspectiva de las relaciones de equivalencia: C es un conjunto de representantes de una relación de equivalencia E sobre X si y sólo si C es un conjunto de representantes de la partición X/E.

Teorema 4.77. Sea E una relación de equivalencia sobre X y sea $C \subseteq X$. Las siguientes afirmaciones son equivalentes:

(a) C es un conjunto de representantes de X/E;

(b) para todo $x \in X$ existe un único $c \in C$ tal que xEc.

Prueba.

(a) → (b) Supongamos que C es un conjunto de representantes de X/E. Esto significa por definición que para toda clase $S \in X/E$, existe $c \in X$ tal que $S \cap C = \{c\}$. Demostremos (ii): sea $x \in X$. Entonces $S = [x] \in X/E$. Luego, por hipótesis, existe $c \in X$ tal que $[x] \cap C = \{c\}$. Entonces $c \in C$ y xEc. Para ver la unicidad de este elemento c, supongamos que c' verifica también que $c' \in C$ y xEc': entonces $c' \in [x] \cap C = \{c\}$, luego $c = c'$.

(b) → (a) Supongamos la afirmación (ii) y demostremos que C es un conjunto de representantes de E. Sea $S \in X/E$. Entonces existe $x \in X$ tal que $S = [x]$. Sea $c \in C$ el único elemento, por (ii), tal que xEc. Esto significa que para todo y tenemos que

$$(y \in C \text{ y } yEx) \text{ si y sólo si } y = c.$$

La anterior equivalencia significa que $S \cap C = \{c\}$. Esto demuestra que C es un conjunto de representantes de la relación E. ∎

☞ **Antes de seguir leyendo**

Sea E una relación de equivalencia sobre X y sea C un conjunto de representantes de E. Demuestre que dados $c_1, c_2 \in C$, se tiene que si $c_1 \neq c_2$, entonces c_1 y c_2 no se encuentran relacionados bajo E.

Ejemplo 4.78.

(a) A es un conjunto de representantes de la relación ID_A. De hecho, A es el único conjunto posible de representantes suyo.

(b) Para la relación de congruencia módulo 2 ($\equiv_2$) sobre $\mathbb{Z}$, los siguientes son distintos conjuntos de representantes: $\{0,1\}$, $\{0,3\}$, $\{-10,5\}$, $\{100,-3\}$, $\{7,6\}$, $\{21,-2\}$, etc. Note que en este caso un conjunto de representantes no es más que un sistema completo de residuos módulo 2 (véase la Definición 3.53).

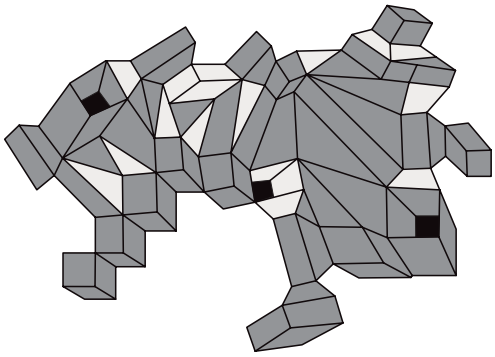
(c) Para la relación E_f (véase el ejemplo 4.67) podemos elegir un conjunto de representantes así: dado $y \in \text{IMG}(f)$, *elegimos* un $x_y \in X$ tal que $f(x_y) = y$. Veamos que el conjunto

$$C = \{x_y : y \in \text{IMG}(f)\} \subseteq X$$

es un conjunto de representantes de E_f. Para $[a] \in X/E_f$, si $b \in [a] \cap C$, entonces $f(b) = f(a)$ y $b = x_y$ para algún $y \in \text{IMG}(f)$. Entonces $f(a) = f(x_y) = y$. Luego $b = x_{f(a)}$. Además, es claro que $x_{f(a)} \in [a] \cap C$, de modo que $[a] \cap C = \{x_{f(a)}\}$.

El lector sospechará que si C es un conjunto de representantes de una partición P, entonces C y P "tienen el mismo tamaño", en algún sentido que será precisado en el capítulo 5.

Ejercicios



1. Sea R una relación sobre X, tal que $\text{DOM}(R) = X$ y R es simétrica y transitiva. Demuestre que R es una relación de equivalencia.
2. Sea $\mathcal{L}$ el conjunto de todas las rectas de $\mathbb{R}^2$. Dé un ejemplo de una relación de equivalencia sobre $\mathcal{L}$, distinta de la relación igualdad.
3. Demuestre que para todo conjunto no vacío X existe una única relación de equivalencia R sobre X tal que X/R es un *singleton*.
4. El siguiente ejercicio es informal, pero ilustrador: sea E el conjunto de puntos de una ciudad donde una persona puede pararse, esto es, el espacio libre de la ciudad (por comodidad, podemos ver a X como un subconjunto de $\mathbb{R}^2$, el plano cartesiano). Definimos la relación $\sim$ sobre E así: pEq si y sólo si es posible ir a pie desde el punto p hacia el punto q.
   (a) Demuestre que $\sim$ es una relación de equivalencia.
   (b) Describa a $[p]$, la clase de un punto p cualquiera.
   (c) Interprete al valor n = tamaño del conjunto $E/\sim$.
5. Sea n un número natural positivo. Dé un ejemplo de una relación de equivalencia R sobre $\mathbb{Z}$ tal que $\mathbb{Z}/R$ sea un conjunto de n elementos.
6. Sea $X = \{0, 1, 2\}$. Calcule el número de relaciones de equivalencia sobre X.

7. Sea $f : X \to Y$ una función sobreyectiva. Definimos la relación E_f sobre X así: aEb si y sólo si $f(a) = f(b)$.
   (a) Demuestre que E_f es una relación de equivalencia.
   (b) Defina una biyección entre X/E_f y Y. (De este modo, la relación E_f "transforma" al conjunto X en un conjunto X/E_f con el mismo tamaño del conjunto Y.)
8. Sea E la relación sobre $\mathbb{Z}$ definida por aEb si y sólo si $a+b$ es par. Demuestre que E es una relación de equivalencia y encuentre un conjunto de representantes de E.
9. Sea R la siguiente relación sobre $\mathbb{R}$: rRs si y sólo si $r - s \in \mathbb{Z}$.
   (a) Demuestre que R es una relación de equivalencia.
   (b) Describa a $[0]$ y a $[\pi]$.
   (c) Demuestre que para $r, s \in \mathbb{R}$: $([r], \leq) \cong ([s], \leq)$. (Para la definición de la relación de isomorfismo, $\cong$, consulte la § 2.4)
   (d) Encuentre un conjunto de representantes de R.
   (e) Concluya que $\mathbb{R}$ es la unión disjunta de copias de $\mathbb{Z}$ (más precisamente, $\mathbb{R}$ puede verse como la unión disjunta de conjuntos isomorfos con el orden a los enteros).
10. Sea E la siguiente relación sobre $\mathbb{R}$: $\theta E \beta$ si y sólo si existe $k \in \mathbb{Z}$ tal que $\theta - \beta = 2\pi k$.
    (a) Demuestre que E es una relación de equivalencia.
    (b) Encuentre cuatro conjuntos distintos de representantes de E.
    (c) Encuentre una biyección entre $\mathbb{R}/E$ y el círculo C dado por $C = \{(x, y) : x^2 + y^2 = 1\}$.
11. Sea $X = \mathbb{R}^2 \setminus \{(0,0)\}$. Definimos la siguiente relación $\sim$ sobre X así: $(a, a') \sim (b, b')$ si y sólo si (a, a') y (b, b') se encuentran ambos sobre una misma recta que pasa por $(0,0)$.
    (a) Demuestre que $\sim$ es una relación de equivalencia.
    (b) Describa geométricamente las clases de la relación $\sim$.
    (c) Encuentre y dibuje un conjunto de representantes de $\sim$.
12. Sea $A = \{n \in \mathbb{N} : 1 < n < 20 \text{ y } n \text{ es divisor de } 20\}$. Sobre A definimos la relación R como

    $$aRb \text{ si y sólo si } a \mid b.$$

    (a) Dibuje la relación (A, R) (como puntos y flechas entre los puntos).
    (b) Demuestre que R es reflexiva pero no simétrica.

(c) ¿Cuál es el mínimo numero de flechas que debemos agregarle al dibujo en (a) para convertir R en una relación de equivalencia? Elabore un nuevo dibujo con la nueva relación.

(d) ¿Cuántas clases de equivalencia tiene la nueva relación?

13. Sean X un conjunto no vacío y E una relación de equivalencia sobre X, tal que E no es la relación identidad. Demuestre que existe más de un conjunto de representantes de E.

14. Sean P una partición sobre X y C un conjunto de representantes de P. Demuestre que existe una función biyectiva $f : C \to P$.

15. Sea E una relación de equivalencia sobre X y sean $C_1, C_2 \subseteq X$ conjuntos de representantes de la relación E. Demuestre que existe una función biyectiva $f : C_1 \to C_2$.

16. Sea $I = [0,1] \subseteq \mathbb{R}$. Entonces I^2 es un cuadrado cuyos lados tienen longitud 1, con borde $B = I^2 \setminus (0,1)^2$. Definimos de esta manera la relación $\sim$ sobre I^2:

$$[(a,b) \sim (c,d)] \leftrightarrow [(a,b),(c,d) \in B \vee (a,b) = (c,d) \notin B].$$

(a) Demuestre que $\sim$ es una relación de equivalencia.

(b) ¿Cuáles son las clases de $\sim$?

(c) Encuentre un conjunto de representantes de $\sim$.

(d) Así como I^2 es un cuadrado, ¿cómo puede verse el conjunto $I^2/\sim$ en términos visuales?

17. Sea E una relación de equivalencia sobre $X = \mathbb{Z}_{10}$. Dados $x, y \in \mathbb{Z}$, decimos que xFy si y sólo si $[x]_{10} E [y]_{10}$.

(a) Demuestre que F es una relación de equivalencia sobre $\mathbb{Z}$.

(b) Suponga que E tiene tres clases de equivalencia. ¿Cuántas tiene F? Justifique claramente su respuesta.

18. Sea E una relación de equivalencia sobre X y F una relación de equivalencia sobre Y. Definimos la siguiente relación $\sim$ sobre $X \times Y$:

$$(x,y) \sim (x',y') \leftrightarrow (xEx' \wedge yFy').$$

(a) Demuestre que $\sim$ es una relación de equivalencia sobre $X \times Y$.

(b) Demuestre que dados $x \in X$ y $y \in Y$, $[(x,y)]_\sim = [x]_E \times [y]_F$.

(c) Demuestre que si $A \subseteq X$ es un conjunto de representantes de E y $B \subseteq Y$ es un conjunto de representantes de Y, entonces $A \times B$ es un conjunto de representantes de $\sim$.

19. Sea X un conjunto finito con n elementos. Dada $f : X \to X$ diremos que f es una *permutación* de X si y sólo si f es una biyección.

Definimos la relación $\sim_f$ sobre X de la siguiente manera: dados $x, y \in X$, $x \sim y$ si y sólo si

$$(x = y) \vee [\exists k \in \mathbb{N}^* : f^{(k)}(x) = y],$$

en donde $f^{(k)}(x)$ denota $\underbrace{(f \circ f \circ \cdots \circ f)}_{k \text{ veces}}(x)$.

(a) Demuestre que $\sim_f$ es una relación de equivalencia sobre X.

(b) Sea $F(f)$ el conjunto de elementos que son dejados fijos por f. Esto es,

$$F(f) \coloneqq \{x \in X : f(x) = x\}.$$

Demuestre que para todo $x \in X$, $x \in F(X)$ si y sólo si $[x] = \{x\}$.

(c) Demuestre que para todo $x \in X$, $[x]$ es un conjunto de la forma

$$\{x_0, \ldots, x_k\},$$

donde $x_0 = x$, $f(x_k) = x_0$ y para todo $i < k$, $f(x_i) = x_{i+1}$. Así, definimos el *ciclo* asociado a $[x]$, y lo denotamos como

$$(x_0 \to x_1 \to \cdots \to x_k)$$

o $f_{[x]}$, como la función $f_{[x]} : X \to X$ dada por: $f_{[x]}(x_i) = x_{i+1}$, $f_{[x]}(x_k) = x_0$ y $f_{[x]}(y) = y$, para $y \in X \setminus [x]$.

(d) Demuestre que para todo $x \in X$ la función $f_{[x]} : X \to X$ es una permutación de X.

(e) Demuestre la *propiedad de descomposición de permutaciones*: si $X / \sim_f$ se compone de r clases, esto es,

$$X / \sim_f = \{[a_0], \ldots, [a_{r-1}]\},$$

entonces $f = f_{[a_0]} \circ \cdots \circ f_{[a_{r-1}]}$. En otras palabras, toda permutación puede escribirse como la composición de sus ciclos.

20. Sea $P \subseteq \mathcal{P}(X)$ una partición de un conjunto X. Demuestre que para $S, S' \subseteq P$ se cumple lo siguiente:

(a) $(\bigcup S) \cup (\bigcup S') = \bigcup (S \cup S')$;

(b) $(\bigcup S) \cap (\bigcup S') = \bigcup (S \cap S')$;

(c) $(\bigcup S)^c = \bigcup (S^c)$. (Aquí $(\bigcup S)^c = X \setminus (\bigcup S)$ y $S^c = P \setminus S$.)

21. Sea $X = \mathcal{P}(\mathbb{N})$. Dados $S, T \in X$ diremos que $S \sim T$ si y sólo si para todo $n \in S$ existe $m \in T$ tal que $n \leq m$, y para todo $n \in T$ existe $m \in S$ tal que $n \leq m$.

(a) Demuestre que $\sim$ es una relación de equivalencia sobre X.

(b) Calcule la clase de $S = \{1, 2, 6\}$.

(c) Describa en detalle las clases de equivalencia de la relación $\sim$.

22. Estudie las igualdades del ejercicio anterior para conjuntos generales, esto es, si $P \subseteq \mathcal{P}(X)$ es un conjunto cualquiera (no necesariamente una partición de X) y $S, S' \subseteq P$, compare:

    (a) $(\bigcup S) \cup (\bigcup S')$ vs. $\bigcup (S \cup S')$,

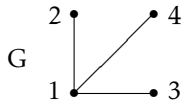
    (b) $(\bigcup S) \cap (\bigcup S')$ vs. $\bigcup (S \cap S')$,

    (c) $(\bigcup S)^c$ vs. $\bigcup (S^c)$. (Aquí $(\bigcup S)^c = X \setminus (\bigcup S)$), y $S^c = P \setminus S$.)

23. Un *grafo* $G = (V, E)$ consiste en un conjunto V de *vértices* junto con una relación binaria $E \subseteq V^2$ irreflexiva y simétrica, llamada el conjunto de *aristas*.[3] A los grafos los representamos por medio de distintos puntos (vértices) unidos por líneas (aristas). Por ejemplo, si $V = \{1, 2, 3, 4\}$ y

$$E = \{(1,4), (4,1), (1,3), (3,1), (1,2), (2,1)\},$$

entonces $G = (V, E)$ es un grafo, que dibujamos de la siguiente manera:



Dados dos grafos $G = (V, E)$ y $G' = (V', E')$, diremos que tales grafos son *isomorfos* (y lo notamos: $G \cong G'$) si y sólo si existe una biyección $f : V \to V'$ tal que para $u, v \in V$, $(u, v) \in E$ si y sólo si $(f(u), f(v)) \in E'$.

(a) Encuentre un grafo isomorfo al grafo de la figura de arriba, tal que su conjunto de vértices sea $V = \{1, 2, 3, 4\}$.

(b) Sea X el conjunto de todos los grafos $G = (V, E)$ no dirigidos sin lazos tales que $V = \{1, 2, 3, 4\}$, y defina en X la siguiente relación: $G = (V, E) \sim G' = (V, E')$ si y sólo si $G \cong G'$.

    (i) Demuestre que la relación $\sim$, tal como ha sido definida, es una relación de equivalencia sobre X.

    (ii) Exhiba un conjunto de representantes de $\sim$ (dibuje estos representantes).

    (iii) ¿Cuántos elementos tiene $X / \sim$? (Si $|X / \sim| = n$, diremos que *existen n grafos distintos de cuatro vértices, módulo isomorfismo*.)

[3] Es posible considerar otro tipo de grafos en donde no se requieran la irreflexividad y la simetría.

24. Sea $G = (V, E)$ un grafo (consulte el ejercicio 23). Dados $x, y \in V$, llamaremos un *camino* entre x y y a una tupla de la forma

$$(x, a_1, a_2, \ldots, a_k, y),$$

en donde

$$xEa_1, a_1Ea_2, \ldots, a_{k-1}Ea_k, a_kEy.$$

Diremos que el grafo G es *conexo* si entre todo par de puntos distintos x y y existe un camino entre ellos.

(a) Sea $G = (V, E)$ el grafo definido por $V = \mathbb{N}$, E la relación dada por xEy si y sólo si $|x - y| \leq 1$. Demuestre que G es un grafo conexo.

(b) Si V es un conjunto finito no vacío con n elementos, ¿cuál es el mínimo número de elementos que debe tener la relación simétrica $E \subseteq V^2$ para que el grafo $G = (V, E)$ sea conexo? Demuestre su respuesta por medio de inducción matemática.

(c) Calcule, módulo isomorfismo, el número de grafos conexos tales que su conjunto de vértices tenga cuatro elementos.

25. Dados los conjuntos $A, B, C \subseteq \mathcal{U}$, diremos que *$A$ y B son iguales módulo C* (en símbolos lo denotamos como $A =_C B$) si y sólo si $A \cap C = B \cap B$.

(a) Demuestre que la relación $=_C$ es una relación de equivalencia sobre $\mathcal{P}(\mathcal{U})$.

(b) Si $\mathcal{U} = \mathbb{N}$, $C = \{1, 2, \ldots, 20\}$ y $A = \{0, 2, 4, \ldots\}$, describa con precisión la clase de A, esto es, $[A] = \{B \subseteq \mathbb{N} : A =_C B\}$.

(c) Describa detalladamente las clases de la relación $=_C$ en términos del conjunto C.

26. Sea $R \subseteq X^2$. Demuestre que las propiedades de reflexividad, simetría y transitividad pueden enunciarse, conjuntistamente, de la siguiente manera:

(a) R es reflexiva si y sólo si $\mathrm{ID}_X \subseteq R$.

(b) R es simétrica si y sólo si $R^{-1} = R$.

(c) R es transitiva si y sólo si $R \circ R \subseteq R$.

27. Dados $a, b \in \mathbb{R}$ con $a < b$, sea $(a, b) = \{x \in \mathbb{R} : a < x < b\}$. Llamaremos *básico* a un conjunto de la forma (a, b). Sea $\mathcal{B}$ el conjunto de todos los básicos, esto es,

$$\mathcal{B} = \{(a, b) : a, b \in \mathbb{R}, a < b\}.$$

Dado un número real cualquiera r, sea $\sim_r$ la siguiente relación sobre $\mathcal{B}$: $(a, b) \sim_r (c, d)$ si y sólo si existe $(y, z) \in \mathcal{B}$ tal que $r \in (y, z)$ y $(a, b) \cap (y, z) = (c, d) \cap (y, z)$.

(a) Demuestre que $\sim_r$ es una relación de equivalencia sobre $\mathcal{B}$.

(b) Demuestre que $[r \in (a,b),(c,d)] \to [(a,b)]_{\sim_r} = [(c,d)]_{\sim_r}$.

(c) Dé un ejemplo de dos básicos (a,b) y (c,d) tales que $r \notin (a,b)$ y $r \notin (c,d)$, pero $[(a,b)]_{\sim_r} \neq [(c,d)]_{\sim_r}$.

(d) ¿Cuántos elementos tiene el conjunto $\mathcal{B}/\sim_r$?

28. Dado X un conjunto y $S \subseteq X$, sea

$$E_S = \{(A,B) \in \mathcal{P}(X) : A \triangle B \subseteq S\}$$

(en donde $A \triangle B = (A \cup B) \setminus (A \cap B)$).

(a) Demuestre que E_S es una relación de equivalencia.

(b) Sean $S, T \subseteq X$. Compare las siguientes parejas de conjuntos:

(i) $E_S \cap E_T$ vs. $E_{S \cap T}$.

(ii) $E_S \cup E_T$ vs. $E_{S \cup T}$.

(iii) $E_S \triangle E_T$ vs. $E_{S \triangle T}$.

29. Sea E una relación sobre X. Demuestre que E es una relación de equivalencia sobre X si y sólo si se cumple la siguiente propiedad:

$$\forall x, y \in X : xEy \leftrightarrow (\forall z \in X : xEz \leftrightarrow yEz).$$

30. Sea X un conjunto y Q una relación sobre X. Definimos $\overline{Q}_{EQ}$ como "la clausura transitiva de la clausura simétrica de la clausura reflexiva de R". Es decir, $\overline{Q}_{EQ}$ es la relación T en donde

$$R := \overline{Q}_{\text{REF}}, \qquad S := \overline{R}_{\text{SIM}}, \qquad T := \overline{S}_{\text{TR}}.$$

(a) Demuestre que T es una relación de equivalencia. (*Ayuda*: utilice el ejercicio 13.)

(b) Demuestre que T es la mínima relación de equivalencia que contiene a Q.

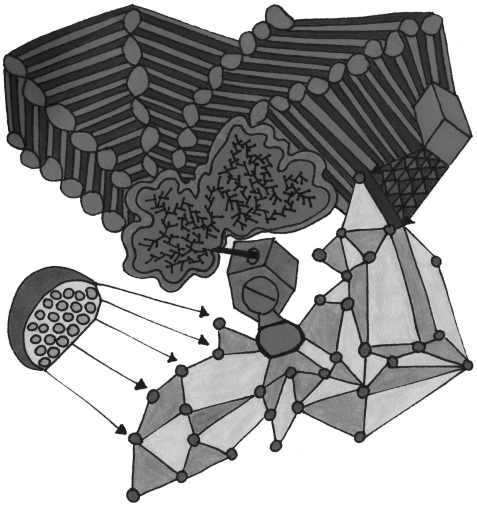
31. Sean X un conjunto y Q una relación sobre X. Diremos que Q es una relación *densa* si $\overline{Q}_{EQ} = X^2$ (véase el ejercicio anterior). Demuestre que las siguientes afirmaciones son equivalentes:

(i) La relación Q es densa.

(ii) Existe una única relación de equivalencia E sobre X, que cumple que $Q \subseteq E$.

(iii) El grafo $G = (X, \overline{Q}_{\text{SIM}})$ es conexo (véase el ejercicio 24).

§ 4.5 Construcción de los números enteros y los racionales



Esta sección constituye una aplicación importante de las relaciones de equivalencia para la construcción de estructuras matemáticas más complejas a partir de otras más simples. En este caso construiremos $\mathbb{Z}$ como un *conjunto bien definido* a partir del conjunto $\mathbb{N}$. Para una definición conjuntista de $\mathbb{N}$, el lector puede consultar el ejercicio 15 de la § 2.2. Después construiremos $\mathbb{Q}$ a partir de $\mathbb{Z}$.

Construcción de los números enteros

Recordemos que el conjunto de los números enteros es

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Sabemos que el orden usual de $\mathbb{Z}$ es el siguiente:

$$\cdots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \cdots.$$

También sabemos sumar estos números: por ejemplo,

$$-3 + -4 = -7,\ 5 + -8 = -3, \text{ etc.}$$

Pues bien, la meta que tenemos en mente es construir la estructura de los números enteros, utilizando la estructura de los números naturales $(\mathbb{N}, \leq, +)$ y la teoría de las relaciones de equivalencia.

Ahora bien, construir la estructura de los números enteros conlleva lo siguiente:

(a) Definir el conjunto $\mathbb{Z}$.

(b) Definir la suma + en el conjunto $\mathbb{Z}$.

(c) Definir el orden $<$ en $\mathbb{Z}$, esto es, dar una condición precisa de cuándo $n < m$, para cualquier par $n, m \in \mathbb{Z}$.

Por supuesto, la multiplicación también forma parte de la estructura de los números enteros, pero por brevedad omitiremos su análisis en esta sección. Tratemos primero de construir los enteros de una manera sencilla e informal. Después el lector comparará este intento con la construcción presentada más adelante, donde verá la elegancia y la naturalidad que tiene el uso de las relaciones de equivalencia para este propósito, aunque en un principio el proceso parezca algo artificial.

(a) *Definición de* $\mathbb{Z}$

$\mathbb{Z} = \mathbb{N} \cup \{-n : n = 1, 2, 3, \dots\}$. En otras palabras, los enteros se componen de los números naturales, más una copia de los números naturales positivos n, acompañados por un "palito" antes, es decir, por el signo $-$, para indicar que son negativos. Por ejemplo, -3 es la copia negativa de 3. A estos números "con palito" los llamaremos *enteros negativos*. Note que $\mathbb{N} \subseteq \mathbb{Z}$.

(b) *Definición de la operación suma*

(i) Para los números enteros naturales, la suma es la misma de los naturales, esto es, la suma de enteros *extiende* a la suma de números naturales.

(ii) Si a, b son ambos negativos, donde $a = -n$ y $b = -m$, con $n, m \in \mathbb{N} \setminus \{0\}$, entonces $a+b$ se define como el número $-(n+m)$, donde este último + denota la suma de números naturales. Por ejemplo, $-4 + -3 = -(4 + 3) = -7$. Esta definición garantiza que la suma de números enteros negativos es un número entero negativo.

(iii) Dejamos al lector la tarea de definir la suma de un número positivo y un número negativo.

(c) *Definición del orden* $<$

(i) Entre números naturales, el orden es el mismo que se tenía en $\mathbb{N}$. En otras palabras, el orden de los números enteros *extiende* al orden de los naturales.

(ii) Si a es un número entero negativo y b es un número natural, entonces $a < b$. Es decir, todo número negativo es menor que todo número no negativo.

(iii) Si a, b son ambos negativos, donde $a = -n$ y $b = -m$, con $n, m \in \mathbb{N}$, entonces $a < b$ si y sólo si $m < n$. Es decir, el los enteros negativos, el orden "se invierte".

Esta definición se resume así:

$$\cdots < -(n+1) < -n < \cdots < -1 < 0 < 1 < \cdots < n < n+1 < \cdots$$

Ahora definiremos el conjunto de los números enteros de una forma notablemente distinta, mediante una relación de equivalencia.

Consideremos el conjunto $\mathbb{N}^2$, que consta de todas las parejas (n, m), con $n, m \in \mathbb{N}$. Imaginemos que cada pareja (n, m) codifica el movimiento vertical de un objeto que se encontraba originalmente en un lugar fijo, en donde n representa el número de unidades que se movió hacia arriba y m el número de unidades que se movió hacia abajo. Por ejemplo, la pareja $(3, 4)$ codifica un movimiento de 3 unidades hacia arriba y después 4 hacia abajo. Es claro que la pareja $(2, 3)$ representa un movimiento distinto al representado por $(3, 4)$. Sin embargo, para efectos de la posición final del objeto, ambos movimientos son *equivalentes*: la localización final de un objeto, ya sea que siga el movimiento $(3, 4)$ o el movimiento $(2, 3)$, será de una unidad bajo el origen, esto es, de -1. Así, cada pareja representará un número entero: $(4, 1)$ representará al entero 3, $(3, 7)$ representará al entero -4, etc. Pero dado que muchas parejas de naturales representan al mismo entero, debemos *meterlas en un mismo barril* y el *barril* será por definición el número entero representado por todos estos elementos.

A continuación formalizamos la discusión anterior.

Definición 4.79. Definimos la relación $\sim$ sobre $\mathbb{N}^2$ del siguiente modo:

$$(n, m) \sim (n', m') \text{ si y sólo si } n + m' = n' + m.$$

Lema 4.80. La relación $\sim$ de la anterior definición es una relación de equivalencia.

Prueba. Se deja al lector (ejercicio 2). ∎

Definición 4.81. Definimos $\mathbb{Z}$, el *conjunto de los números enteros*, así:

$$\mathbb{Z} := \mathbb{N}^2 / \sim = \{[(n, m)] : (n, m) \in \mathbb{N}^2\}.$$

$\underline{n}$
$\underline{-n}$

Definición 4.82. Dado $n \in \mathbb{N}$, definimos los siguientes números enteros (los escribimos subrayados para enfatizar que son números enteros):

$$\underline{n} := [(n, 0)] \in \mathbb{Z}; \qquad \underline{-n} := [(0, n)] \in \mathbb{Z}.$$

Técnicamente, el número entero $\underline{2}$ es *distinto* del número natural 2. Por ejemplo, $\underline{-6} = [(0,6)] = [(1,7)] = [(5,11)]$ y, si $a = [(3,5)]$, entonces

$$a = [(3,5)] = [(2,4)] = [(1,3)] = [(0,2)] = \underline{-2}.$$

Por definición, diremos que un número entero $a \in \mathbb{Z}$ es *positivo* si es de la forma $\underline{n}$, en donde $n \in \mathbb{N}^*$; diremos que a es *negativo* si éste es de la forma $\underline{-n}$, en donde $n \in \mathbb{N}^*$.

Entero positivo

Entero negativo

☞ **Antes de seguir leyendo**

1. Demuestre que $[(7,13)]$ es un número entero negativo.
2. Demuestre que para todo $a \in \mathbb{Z}$ se tiene que a es positivo si y sólo si para todo $(n,m) \in a$, $m \leq n$.

Antes de continuar es necesario introducir el concepto de *buena definición* de operaciones o relaciones, que es fundamental cuando se quieren definir nuevas relaciones u operaciones sobre conjuntos cociente, esto es, conjuntos de la forma $X/\sim$, donde $\sim$ es una relación de equivalencia sobre X.

Supongamos, por ejemplo, que se nos da lo siguiente: sea $g : \mathbb{N}^2 \to \mathbb{N}$ la función dada por $g(n,m) = n+m$. Ahora, a partir de la función g, cuyo dominio es $\mathbb{N}^2$, sería natural definir una función $\hat{g} : \mathbb{N}^2/\sim \to \mathbb{N}$ de la siguiente manera: $\hat{g}([(n,m)]) = g(n,m)$.

El problema con la anterior definición de $\hat{g}$ es que es ambigua, es decir, $\hat{g}$ no es una función. Por ejemplo, sea $a = [(3,4)]$. Según esto, $\hat{g}(a) = 3+4 = 7$. Sin embargo, dado que $(3,4) \sim (5,6)$, tenemos que $a = [(3,4)] = [(5,6)]$ y por esto $\hat{g}(a) = \hat{g}([(5,6)]) = g(5,6) = 5+6 = 11$. Entonces $\hat{g}(a)$ no está bien definida, esto es, el valor de $\hat{g}(a)$ *depende* del representante (n,m) de la clase a que se tome y, por tanto, $\hat{g}$ no es una función.

Naturalmente, quisiéramos definir la suma en $\mathbb{Z}$ de modo que coincida con la suma que ya conocemos y utilizamos cotidianamente en los números enteros. Por ejemplo, quisiéramos que al sumar $\underline{2}$ con $\underline{-6}$ el resultado fuera $\underline{-4}$. Según nuestras definiciones, el número entero $\underline{2}$ es la clase de la pareja $(5,3)$, esto es, $\underline{2} = [(5,3)]$. De modo similar, $\underline{-6} = [(1,7)]$. Notemos que si sumamos las parejas $(5,3)$ y $(1,7)$ "componente por componente", obtenemos la pareja $(5+1, 3+7) = (6,10)$. Pero la clase de $(6,10)$ es $[(6,10)] = [(0,4)]$, que es precisamente $\underline{-4}$.

Si en vez de utilizar los representantes $(5,3)$ y $(1,7)$ de $\underline{2}$ y $\underline{-6}$ respectivamente utilizamos otros representantes y los sumamos componente a componente, ¿obtenemos también un representante de $\underline{-4}$? Tomemos,

por ejemplo, $(3,1) \in \underline{2}$ y $(4,10) \in \underline{-6}$. Si sumamos estas parejas componente por componente, obtenemos $(3+4, 1+10) = (7,11)$. La clase de $(7,11)$ es $\underline{-4}$. Note que antes habíamos obtenido la pareja $(6,10)$, y ahora obtenemos a una pareja distinta $(7,11)$, pero $(6,10) \sim (7,11)$. Esto es, en esencia obtenemos la misma clase de equivalencia, a saber, $\underline{-4} = \{(0,4),(1,5),(2,6),\dots\}$.

Suma de números enteros

Lo anterior motiva a definir de la suma de números enteros de la siguiente manera:

$$[(n,m)] + [(n',m')] := [(n+n', m+m')].$$

Note que el primer símbolo de suma denota la suma de números enteros que estamos definiendo, y los símbolos de suma a la derecha de la igualdad denotan la suma en los números naturales, que aceptamos como ya definida. Para evitar esta ambigüedad, sea $f : \mathbb{N}^2 \times \mathbb{N}^2 \to \mathbb{N}^2$ la función dada por

$$f((n,m),(n',m')) = (n+n', m+m').$$

A partir de esta función definimos $\hat{f}$ así:

$$\begin{aligned} \hat{f} : (\mathbb{N}^2/\sim) \times (\mathbb{N}^2/\sim) &\to (\mathbb{N}^2/\sim) \\ ([(n,m)],[(n',m')]) &\mapsto [f((n,m),(n',m'))]. \end{aligned}$$

¿Se encuentra $\hat{f}$ bien definida? Para verificar que es así, debemos demostrar que si

$$(n_1,m_1) \sim (n_2,m_2) \text{ y } (n_1',m_1') \sim (n_2',m_2'),$$

entonces se tiene que

$$f((n_1,m_1),(n_1',m_1')) \sim f((n_2,m_2),(n_2',m_2')),$$

es decir, que

$$[f((n_1,m_1),(n_1',m_1'))] = [f((n_2,m_2),(n_2',m_2'))].$$

El ejemplo anterior es un caso particular de este hecho general, que hemos de probar, en donde:

$$\begin{aligned} (n_1,m_1) = (5,3), (n_2,m_2) = (3,1) &\sim (5,3); \\ (n_1',m_1') = (1,7), (n_2',m_2') = (4,10) &\sim (1,7); \\ f((n_1,m_1),(n_1',m_1')) &= (6,10); \\ f((n_2,m_2),(n_2',m_2')) &= (7,11) \sim (6,10). \end{aligned}$$

Lema 4.83. La definición de $\hat{f}$ dada arriba es una buena definición. En otras palabras, si $(n_1,m_1) \sim (n_2,m_2)$ y $(n_1',m_1') \sim (n_2',m_2')$, entonces

$$f((n_1,m_1),(n_1',m_1')) \sim f((n_2,m_2),(n_2',m_2')).$$

Prueba. Se deja al lector (ejercicio 3). ∎

Por ejemplo, para sumar los números enteros $\underline{-5}$ y $\underline{-8}$, tomamos *cualquier* representante $(n,m) \in \underline{-5}$ y *cualquier* representante $(n',m') \in \underline{-8}$, sumamos estas parejas componente por componente, esto es, calculamos $f((n,m),(n',m'))$ y *la clase* del resultado es por definición el número entero $\underline{-5} + \underline{-8}$. Hagamos esto: tomamos $(2,7) \in \underline{-5}$, $(1,9) \in \underline{-8}$. Tenemos que $f((2,7),(1,9)) = (3,16)$. Entonces

$$\underline{-5} + \underline{-8} = [(3,16)] = [(2,15)] = [(1,14)] = [(0,13)] = \underline{-13}.$$

Sumersión de $\mathbb{N}$ en $\mathbb{Z}$

Definimos el conjunto $\underline{\mathbb{N}}$ así:

$$\underline{\mathbb{N}} := \{\underline{n} : n \in \mathbb{N}\}.$$

Es decir, $\underline{\mathbb{N}} = \{\underline{0},\underline{1},\underline{2},\dots\} = \{[0,0],[1,0],[2,0],\dots\} \subseteq \mathbb{Z}$. Para facilitar las cosas, en esta sección llamaremos *naturales viejos* a los elementos del conjunto $\mathbb{N}$ y *naturales nuevos* a los elementos del conjunto $\underline{\mathbb{N}}$.

¿Cuán distintos son los naturales nuevos de los naturales viejos? Como conjunto son distintos. Sin embargo, como estructuras, son isomorfas: los nuevos naturales tienen exactamente la misma estructura de los naturales viejos, en cuanto a la suma y la multiplicación. Definamos el producto en los naturales nuevos de la forma esperada, esto es, $[(n,0)][(m,0)] := [(nm,0)]$. Aquí nm denota el producto entre los naturales viejos n y m, que consideramos ya definido. Por ejemplo, la operación $(4)(5) = 20$ en los naturales viejos, se *traduce* en la operación

$$[(4,0)][(5,0)] = [((4)(5),0)] = [(20,0)],$$

que es esencialmente la misma. Si la identidad de la multiplicación en los naturales viejos es el número 1, entonces en los naturales nuevos será $[(1,0)]$, ya que para todo número natural nuevo $[(n,0)]$, se tiene que

$$[(1,0)][(n,0)] = [(1n,0)] = [(n,0)].$$

Consideremos un número natural viejo cualquiera, digamos, el 3. Estrictamente $3 \notin \mathbb{Z}$, pero $\underline{3}$, su "copia nueva", sí pertenece a $\mathbb{Z}$. Dicho de otro modo, el conjunto $\mathbb{N}$ no es un subconjunto de $\mathbb{Z}$, mientras que $\underline{\mathbb{N}}$ sí lo es. La estructura de los números naturales viejos "vive" en $\mathbb{Z}$, gracias a una copia, a saber, los números naturales nuevos. Además, la estructura de la suma en $\underline{\mathbb{N}}$ funciona esencialmente igual a como funcionaba en $\mathbb{N}$: por ejemplo, $3 + 4 = 7$ y, como es fácil ver, $\underline{3} + \underline{4} = \underline{7}$.

Para formalizar lo anterior, definimos la función "copia" $\alpha : \mathbb{N} \to \mathbb{Z}$ así: $\alpha(n) = \underline{n} = [(n,0)]$. Entonces tenemos que

(a) α es una función inyectiva;

(b) dados $n,m \in \mathbb{N}$ se tiene que $\alpha(n+m) = \alpha(n) + \alpha(m)$.

Verifiquemos la inyectividad de α: supongamos que $\alpha(n) = \alpha(m)$, esto es, $[(n,0)] = [(m,0)]$, así que $(n,0) \sim (m,0)$ o, lo que es lo mismo, $n + 0 = m + 0$, luego $n = m$.

Para demostrar que la imagen de la suma bajo α es la suma de las imágenes bajo α, basta observar que

$$\alpha(n+m) = [(n+m,0)] = [(n,0)] + [(m,0)] = \alpha(n) + \alpha(m).$$

La segunda igualdad vale gracias a la definición de la suma de números enteros.

Sumersión

Como la función α cumple con las condiciones (a) y (b), diremos que α es una *sumersión* de los naturales viejos en los números enteros (α es una sumersión de $\mathbb{N}$ en $\mathbb{Z}$). Además, es claro que $\text{IMG}(\alpha) = \underline{\mathbb{N}}$.

Quisiéramos que los números naturales fueran también números enteros. Para lograr esto abusaremos del lenguaje e identificaremos cada número natural viejo n con su copia $\underline{n}$: esto es: "$n = \underline{n}$". Tal identificación, aunque estrictamente es incorrecta —pues, por ejemplo, 5 y $[(5,0)]$ son dos objetos distintos—, no es nociva en absoluto; de hecho, es tremendamente pragmática y facilita las cosas, pues cuando sumemos números enteros, en vez de escribir, por ejemplo,

$$(\underline{2} + \underline{13}) + \underline{8} = \underline{23},$$

simplemente escribiremos

$$(2 + 13) + 8 = 23.$$

Al identificar cada n con $\underline{n}$, automáticamente identificamos al conjunto $\mathbb{N}$ con $\underline{\mathbb{N}}$: "$\mathbb{N} = \underline{\mathbb{N}}$". En otras palabras, los nuevos naturales han reemplazado a los viejos naturales. Esto tiene como consecuencia que *ahora* los números naturales son clases de equivalencia:

Redefinición de $\mathbb{N}$.

$$\mathbb{N} := \{[(0,0)], [(1,0)], [(2,0)], \dots\}.$$

Esta igualdad permite concluir, *ahora sí*, que $\mathbb{N} \subseteq \mathbb{Z}$.

Definición 4.84. Dado $a = [(n,m)] \in \mathbb{Z}$, definimos $-a := [(m,n)]$.

Lema 4.85. La función $-$ está bien definida, esto es, no depende del representante (n,m). Más precisamente, dados $(n,m), (n',m') \in a$, se tiene que $[(m,n)] = [(m',n')]$.

Prueba. Sean $(n,m), (n',m') \in a$. Como (n,m) y (n',m') pertenecen a la misma clase, entonces son equivalentes bajo $\sim$, esto es, $n + m' = n' + m$. Esto implica trivialmente, gracias a la conmutatividad de la suma, que $m + n' = m' + n$, lo que implica por definición que $(m,n) \sim (m',n')$. Por lo tanto, $[(m,n)] = [(m',n')]$ ∎

Es usual llamar a $-$ la operación unaria del *inverso aditivo*, ya que verifica la siguiente propiedad:

Lema 4.86. Para todo $a \in \mathbb{Z}, a + -a = 0$.

Prueba. Empecemos por recordar que $0 = [(0,0)]$, según la identificación de naturales viejos con naturales nuevos. Sea ahora $a = [(n,m)]$. Entonces $-a = [(m,n)]$, luego $a + -a = [(n+m, m+n)]$. Pero claramente se tiene que $(n+m, m+n) \sim (0,0)$, lo que implica que $a + -a = [(0,0)] = 0$. ∎

$-a$: Inverso aditivo

Al número entero $-a$ lo llamaremos el *inverso aditivo de a*. Además, se tiene que todo elemento $a \in \mathbb{Z}$ tiene un (único) inverso aditivo, esto es, un elemento $b \in \mathbb{Z}$ tal que $a + b = 0$. Esto no ocurre en general en los números naturales. Por ejemplo, $8 + n \neq 0$ para cualquier natural n. Intuitivamente, una vez "nos encontremos" en 8, no podemos invertir la dirección y devolvernos al 0, utilizando números naturales. Para ello es necesario extender los naturales a los enteros, en donde hay *bidireccionalidad*.

A continuación hacemos una observación sutil. Recordemos que, dado un número natural viejo n, el número entero $\underline{-n}$ se definió como $[(0,n)]$. Ahora, dado que $\underline{n} = [(n,0)]$, concluimos —gracias a la Definición 4.84— que $\underline{-n} = -\underline{n}$. Dado que estamos identificando a $\underline{n}$ con n, concluimos que

$$-n = -\underline{n} = \underline{-n} = [(0,n)].$$

Por ello tiene sentido referirse al entero $-n$. Por ejemplo, $-5 = [(0,5)]$.

☞ **Antes de seguir leyendo**

1. Demuestre que para todo $(n,m) \in \mathbb{N}^2$ existe un número natural k tal que $(n,m) \sim (k,0)$ o $(n,m) \sim (0,k)$. (*Ayuda*: utilice inducción en n o en m.)
2. Utilice dicha propiedad para demostrar que para todo $a \in \mathbb{Z}$ existe un único número natural k tal que $a = [(k,0)] = k$ (la última igualdad vale por convención), o bien $a = [(0,k)] = -k$ (la última igualdad vale también por convención). Concluya que $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\}$. Es decir, todo número entero es un número natural o un número negativo, esto es, un número de la forma $-n$ donde n es un número natural distinto de 0.
3. Demuestre que la suma de números enteros es conmutativa.
4. Demuestre que $0 = [(0,0)]$ es la identidad bajo la suma, esto es, que para todo $a \in \mathbb{Z}$ tenemos que $0 + a = a + 0 = a$, y que además 0 es el *único* número entero con esta propiedad.

Ahora definimos el orden $<$ en $\mathbb{Z}$ así:

$$[(n,m)] < [(n',m')] \text{ si y sólo si } n+m' < n'+m,$$

en donde el símbolo $<$ de la derecha denota el orden en los números naturales viejos, el cual aceptamos como ya definido.

Quien acaba de leer el anterior párrafo tal como está escrito debe hacer una pausa y reflexionar sobre lo que significa. Es conveniente que el lector matemático desarrolle una actitud crítica sobre lo que lee respecto a la *motivación* y al *rigor*. En el caso del párrafo anterior, un lector crítico se hará de manera natural las siguientes preguntas:

1. ¿Por qué se está definiendo el orden en los enteros de esta manera?
2. ¿Es fácil encontrar un ejemplo que sugiera que esta definición va en la dirección correcta?
3. ¿Coincide este orden con el orden ya definido de los naturales, haciendo la identificación $n = \underline{n}$?
4. ¿Es esta una definición libre de ambigüedad? ¿Depende o no de los representantes que elijamos?

Antes de continuar leyendo, le recomendamos al lector intentar responder cada una de estas preguntas.

La motivación para definir el orden como arriba es esta: si $a = [(n,m)]$ y $a' = [(n',m')]$, entonces a representa la posición final después de moverse n unidades hacia arriba y m hacia abajo, y algo similar sucede con a'. Para decidir si a representa una posición más baja que a', observamos que cuanto más grande sean n y m', tanto más arriba quedará a respecto de a'; y cuanto más grande sean m y n', tanto más arriba quedará a' respecto a a. Así, es razonable afirmar que a quedará más abajo que a' si y sólo si la cantidad $n+m'$ es menor que la cantidad $n'+m$. El lector podrá dar varios ejemplos que ilustren el razonamiento anterior.

Esto último también puede expresarse mediante ecuaciones de la siguiente manera: sean $a = [(n,m)]$ y $a' = [(n',m')]$. Entonces se tiene que $a = n - m$, $a' = n' - m'$, y además

$$a < a' \leftrightarrow n - m < n' - m' \leftrightarrow n + m' < n' + m.$$

Note que la anterior línea no es una demostración, sino una motivación no rigurosa pero poderosa para darle sentido a la definición que hemos dado.

Pasemos ahora a la cuestión del rigor. Debemos demostrar que la definición del orden es *buena*, esto es, que verificar si $a < a'$ no depende de los representantes que escojamos en cada clase. Más precisamente, debemos verificar lo siguiente: dados $(n_1,m_1),(n_2,m_2) \in a$ y $(n_1',m_1'),(n_2',m_2') \in a'$, si $n_1 + m_1' < n_1' + m_1$, entonces $n_2 + m_2' < n_2' + m_2$.

Si verificamos lo anterior, entonces la pregunta por si $a < a'$ se resolverá afirmativamente para *toda* elección de representantes en a y a'; en este caso diremos que $a < a'$. O bien se resolverá negativamente para *toda* elección de representantes en a y a', y en este caso diremos que $a \not< a'$; pero no ocurrirá que se resuelva afirmativamente para algunos representantes y negativamente para otros. Demostremos, entonces, la buena definición de $<$.

Lema 4.87. La definición del orden $<$ en $\mathbb{Z}$ es una buena definición.

Prueba. Sean $a, a' \in \mathbb{Z}$ y sean $(n_1, m_1), (n_2, m_2) \in a$ y $(n_1', m_1'), (n_2', m_2') \in a'$. Supongamos que $n_1 + m_1' < n_1' + m_1$. Si sumamos $m_2 + m_2'$ a cada lado preservamos la desigualdad, pues esta es una propiedad del orden $<$ en los naturales; y si la reorganizamos, obtenemos lo siguiente:

$$n_1 + m_2 + m_2' + m_1' < n_1' + m_2' + m_2 + m_1.$$

Ahora, como (n_1, m_1) y (n_2, m_2) pertenecen a la misma clase, entonces $(n_1, m_1) \sim (n_2, m_2)$, es decir, $n_1 + m_2 = n_2 + m_1$. De manera similar, podemos concluir que $n_1' + m_2' = n_2' + m_1'$. Gracias a estas igualdades, la anterior desigualdad se transforma en

$$n_2 + m_1 + m_2' + m_1' < n_2' + m_1' + m_2 + m_1.$$

Como en ambos lados de la desigualdad aparece $m_1 + m_1'$, concluimos, por las propiedades del $<$ en los números naturales, que

$$n_2 + m_2' < n_2' + m_2. \qquad \blacksquare$$

Recordemos que un número entero negativo es por definición un número entero de la forma $[(0, k)]$, con $k > 0$. El contenido del siguiente teorema es bien conocido:

Teorema 4.88. Sean $a, a' \in \mathbb{Z}$. Si $a \in \mathbb{N}$ y a' es negativo, entonces $a' < a$.

Prueba. Sea $a = [(k, 0)]$, $a' = [(0, k')]$. Puesto que a' es negativo, $k' > 0$. Esto implica que $0 + 0 < k + k'$, lo que a su vez implica que $a' < a$. $\blacksquare$

☞ **Antes de seguir leyendo**

Demuestre las siguientes afirmaciones:

1. Para todo $b \in \mathbb{Z}$ existe $a \in \mathbb{Z}$ tal que $a < b$.
2. Para $a, b \in \mathbb{Z}$, $a < b$ si y sólo si $-b < -a$.
3. Para $a, b, c \in \mathbb{Z}$, si $a < b$ y $b < c$, entonces $a < c$.

No es nuestro objetivo demostrar las principales propiedades del orden en $\mathbb{Z}$. Sin embargo, es bueno preguntarse cómo se compara el orden en el conjunto de los números naturales con el orden en el conjunto de los números enteros: ¿qué propiedades se preservan en $\mathbb{Z}$ y dónde hay una ruptura estructural con respecto de $\mathbb{N}$? A continuación listamos las principales semejanzas y diferencias. Para ello llamamos $<_{\mathbb{N}}$ al orden en los naturales y $<_{\mathbb{Z}}$ al orden en los enteros.

1. Ambos órdenes carecen de un elemento máximo.
2. Ambos órdenes son "discretos hacia arriba", esto es, todo elemento tiene un sucesor inmediato. (Note que esto no ocurre en el conjunto $\mathbb{Q}$ de los números racionales.)
3. La relación $<_{\mathbb{N}}$ es un buen orden, mientras que $<_{\mathbb{Z}}$ no lo es (es por ello que no podemos hacer inducción en el orden los enteros).
4. El orden $(\mathbb{N}, <_{\mathbb{N}})$ es *rígido*. En otras palabras, el único isomorfismo $\alpha : (\mathbb{N}, <_{\mathbb{N}}) \cong (\mathbb{N}, <_{\mathbb{N}})$ es la función identidad. Por el contrario, $(\mathbb{Z}, <_{\mathbb{Z}})$ no es una *estructura rígida*,[4] esto es, existe un isomorfismo $\alpha : (\mathbb{Z}, <_{\mathbb{Z}}) \cong (\mathbb{Z}, <_{\mathbb{Z}})$ tal que α es distinto de la identidad.

Estructuras rígidas

☞ Antes de seguir leyendo

1. Encuentre un isomorfismo $\alpha : \mathbb{Z} \cong \mathbb{Z}$ tal que α no sea la función identidad, esto es, tal que $\alpha(a) \neq a$ para por lo menos algún $a \in \mathbb{Z}$. (Para la noción de isomorfismo, consulte la § 2.4, arriba.)
2. ¿Cómo definiría la multiplicación entre números enteros? Verifique que su definición no sea ambigua y, mediante ejemplos, verifique que coincida con la multiplicación usual en los enteros.
3. Verifique que la definición de multiplicación dada en el numeral anterior es conmutativa.

Construcción de los números racionales

En este apartado construiremos el conjunto $\mathbb{Q}$ de los números racionales a partir del conjunto de los números enteros.

Desde temprano nos han enseñado que una fracción admite representaciones distintas. Por ejemplo, las fracciones $\frac{2}{3}$ y $\frac{10}{15}$ *son* el mismo número, aunque representado de dos formas distintas. Esto es, $\frac{2}{3} = \frac{10}{15}$.

[4] Una estructura se dice *rígida* si el único isomorfismo entre ella y sí misma es la función identidad.

¿Es posible expresar esta igualdad sin hacer uso de la división o el cociente, ya que es lo que queremos definir? Resulta que sí. Tal igualdad es equivalente a la siguiente:

$$(2)(15) = 30 = (10)(3).$$

Si generalizamos el caso considerado, podemos entonces afirmar que dos representaciones de fracciones $\frac{a}{b}$ y $\frac{a'}{b'}$ serán "equivalentes", o denotarán el mismo número racional, si y solamente si $ab' = a'b$.

Sea $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Definimos la relación $\sim$ sobre el conjunto $X = \mathbb{Z} \times \mathbb{Z}^*$ de la siguiente forma:

$$(a,b) \sim (a',b') \text{ si y sólo si } ab' = a'b.$$

Lema 4.89. La relación $\sim$ es una relación de equivalencia sobre X.

Prueba. Se deja al lector (ejercicio 4). ∎

Definimos al conjunto de los números racionales así: $\mathbb{Q} := X/\sim$. Dados $a, b \in \mathbb{Z}$ con $b \neq 0$, definimos la fracción $\frac{a}{b}$ así:

$$\frac{a}{b} = [(a,b)].$$

Por ejemplo, $\frac{4}{5} = [(4,5)] = [(8,10)]$. Además, todo número entero puede verse como un número racional: por ejemplo, el número entero 5 será ahora el número racional $[(5,1)]$. En general, todo "entero viejo" z se identificará con el racional $\underline{z} := [(z,1)]$. Esto es análogo a lo que hicimos en la construcción de los enteros, donde sumergimos $\mathbb{N}$ en $\mathbb{Z}$.

Las operaciones y relaciones conocidas en el conjunto de los números racionales (esto es, $+$, $<$ y $\cdot$) pueden definirse en términos de las conocidas en el conjunto de los números enteros.

Definición 4.90 (Estructura de los números racionales). Dados $[(a,b)], [(a',b')] \in \mathbb{Q}$, definimos:

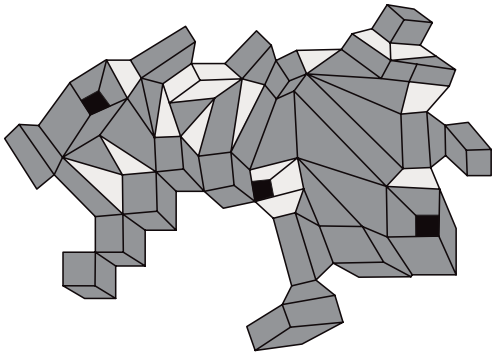
(a) *suma*: $[(a,b)] + [(a',b')] := [(ab' + a'b, bb')]$;

(b) *producto*: $[(a,b)] \cdot [(a',b')] := [(aa', bb')]$;

(c) *orden*: $[(a,b)] < [(a',b')]$ si y sólo si $(ab' - a'b)bb' < 0$.

En el ejercicio 5 se pide al lector demostrar que estas definiciones son en realidad buenas definiciones. Un buen reto para el lector consiste en descubrir por qué éstas se definen de este modo. Para ello es recomendable pensar en algunos ejemplos.

Ejercicios



1. Demuestre que para todo $a, b \in \mathbb{Z}$ se cumplen las siguientes propiedades:
   (a) $-(-a) = a$;
   (b) $a + -a = 0 = -a + a$;
   (c) $-(a + b) = -a + -b$.
2. Demuestre el Lema 4.80.
3. Demuestre el Lema 4.83.
4. Demuestre el Lema 4.89.
5. Demuestre que las operaciones y relaciones de la Definición 4.90 están bien definidas.

§ 4.6 Conteo mediante relaciones de equivalencia

En esta sección utilizaremos las funciones biyectivas y las relaciones de equivalencia como un poderoso instrumento para calcular el tamaño de ciertos conjuntos. Para comenzar, necesitamos el siguiente lema:

Lema 4.91. Sea $n \in \mathbb{N}$. Si A es un conjunto tal que $|A| = n$ (véanse las definiciones 2.24 y 2.25) y $f : A \to B$ es una biyección, entonces $|B| = n$.

Prueba. La demostración se puede hacer mediante inducción en n y se deja al lector (ejercicio 1). ∎

Como podemos notar, el lema anterior se encuentra ejemplificado en el apartado *Antes de seguir leyendo* que sigue a la Definición 4.43: la

existencia de una biyección entre dos conjuntos finitos es evidencia de que éstos tienen el mismo tamaño.[5]

Recordemos que $\mathcal{P}_k(A)$ es el conjunto de los subconjuntos de A que tienen tamaño k. En el capítulo 2 (Corolario 2.30) demostramos que si $|A| = n \in \mathbb{N}$, entonces

$$|\mathcal{P}_2(A)| = \frac{n(n-1)}{2}.$$

Si A tiene n elementos, ¿cuál es el tamaño del conjunto $|\mathcal{P}_k(A)|$ en términos de k y de n? El siguiente teorema responde a esta inquietud de forma precisa:

Teorema 4.92. Sean $k, n \in \mathbb{N}$ con $k \leq n$ y sea A un conjunto tal que $|A| = n$. Entonces se tiene que

$$|\mathcal{P}_k(A)| = \frac{n!}{k!(n-k)!}.$$

Prueba. El caso $k = 0$ es sencillo (pues $0! = 1$). Supongamos entonces que $k \geq 1$. Recordemos que

$$A!(k) := \{(a_1, \ldots, a_k) \in A^k : \ a_s \neq a_t \text{ para todo } s \neq t\}.$$

Definimos la siguiente función $f : A!(k) \to \mathcal{P}_k(A)$:

$$f((a_1, \ldots, a_k)) = \{a_1, \ldots, a_k\}.$$

Esta función es evidentemente sobreyectiva. Sea $\sim$ la relación de equivalencia sobre $A!(k)$ determinada por f, es decir, dados $\vec{a}, \vec{b} \in A!(k)$,

$$\vec{a} \sim \vec{b} \text{ si y sólo si } f(\vec{a}) = f(\vec{b}).$$

Hacemos las siguientes observaciones:

(i) Si $P \in A!(k)/\sim$, entonces $|P| = k!$: si $P = [(a_1, \ldots, a_k)]$, entonces P consta de todas las tuplas de longitud k formadas por $a_1, \ldots, a_k$ que no repiten entradas y el número de estas tuplas es $k!$ (véase el Teorema 2.35 (c)).

(ii) El número de elementos de $\mathcal{P}_k(A)$ es igual al número de elementos de $A!(k)/\sim$: definamos la función

$$g : A!(k)/\sim \to \mathcal{P}_k(A)$$

del siguiente modo:

$$g([\vec{a}]) = f(\vec{a}) \qquad (\vec{a} \in A!(k)).$$

Es fácil verificar que la función g está bien definida, puesto que si $\vec{a} \sim \vec{b}$, entonces por definición $f(\vec{a}) = f(\vec{b})$.

[5] En general, la existencia de una biyección entre dos conjuntos, finitos o infinitos, será la *definición oficial* de que tienen el mismo tamaño. Esto lo estudiaremos con más detalle en el capítulo 5.

Veamos que g es una biyección:

(a) *Inyectividad*: si $g([\vec{a}]) = g([\vec{b}])$, entonces $f(\vec{a}) = f(\vec{b})$. Luego $\vec{a} \sim \vec{b}$ y, por ende, $[\vec{a}] = [\vec{b}]$.

(b) *Sobreyectividad*: sea $B = \{b_1, \ldots, b_k\} \in \mathcal{P}_k(A)$. Entonces es claro que $g([(b_1, \ldots, b_k)]) = B$.

Por el Lema 4.91, concluimos que $|\mathcal{P}_k(A)| = |A!(k)/\sim|$.

(iii) $|A!(k)/\sim| = \frac{n!}{k!(n-k)!}$: sabemos que $|A!(k)| = \frac{n!}{(n-k)!}$ (Teorema 2.34) y además, por la observación (i), para toda clase $P \in A!(k)/\sim$ se tiene que $|P| = k!$. Podemos aprovechar este hecho para plantear la siguiente ecuación:[6]

$|A!(k)| =$ (N° de clases de equivalencia)(tamaño de cada clase).

Es decir,

$$\frac{n!}{(n-k)!} = |A!(k)/\sim| \cdot k!.$$

Entonces

$$|A!(k)/\sim| = \frac{n!}{k!(n-k)!}.$$

Por las observaciones (ii) y (iii), concluimos que

$$|\mathcal{P}_k(A)| = \frac{n!}{k!(n-k)!}.$$ ∎

$\binom{n}{k}$: *coeficiente binomial*

Definición 4.93 (Coeficiente binomial). Sean $k, n \in \mathbb{N}$ con $k \leq n$ y sea A un conjunto con n elementos. Definimos el *coeficiente binomial* $\binom{n}{k}$ como

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$

Note que, por el Teorema 4.92, $|\mathcal{P}_k(A)| = \binom{n}{k}$.

Ejemplo 4.94. Sea $A = \{1, 2, 3, 4, 5, 6\}$. Determine el número de subconjuntos de A cuyo tamaño es igual a 4.

Solución. Simplemente calculamos

$$\binom{6}{4} = \frac{6!}{4!(6-4)!} = \frac{(6)(5)}{2} = 15.$$

[6] Esta ecuación será válida cuando todas las clases de equivalencia tienen el mismo tamaño, el cual no siempre es el caso.

☞ **Antes de seguir leyendo**

1. Sea $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Determine el número de subconjuntos de A cuyo tamaño es par.
2. Demuestre que $\binom{n}{k} = \binom{n}{n-k}$.
3. Demuestre que $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$.

Ejemplo 4.95. Cuando decimos *palabra* en este ejemplo no requerimos que ésta aparezca en el diccionario, sino sencillamente que sea una sucesión ordenada de letras. Determine cuántas palabras distintas de longitud 7 pueden hacerse con las siguientes fichas de letras (podemos pensar que son fichas del conocido juego Scrabble):

$$[M], [A], [N], [A], [D], [A], [S].$$

Solución. Sea $\mathcal{B}$ el conjunto de todas las palabras de longitud siete formadas utilizando las fichas anteriores. Queremos averiguar el tamaño de este conjunto. Supongamos primero que las fichas de la [A] son distintas entre sí y sean ellas $[A_1]$, $[A_2]$ y $[A_3]$. En estas condiciones podemos formar 7! palabras distintas. Sea $\mathcal{C}$ el conjunto de todas estas palabras. Definimos la siguiente relación de equivalencia $\sim$ sobre $\mathcal{C}$: dadas dos palabras $c, d \in \mathcal{C}$, $c \sim d$ si y sólo si al remover los subíndices de las A-es en c y d obtenemos la misma palabra. Por ejemplo, si

$$c = [A_1][A_3][M][D][A_2][S][N], \quad \text{y}$$
$$d = [A_3][A_1][M][D][A_2][S][N],$$

entonces $c \sim d$, ya que al remover los subíndices de las Aes obtenemos la misma palabra, a saber,

$$[A][A][M][D][A][S][N].$$

Dejamos al lector la tarea de verificar que la relación $\sim$ es una relación de equivalencia en la que toda clase de equivalencia tiene exactamente 3! elementos. Ahora, tenemos que

$$|\mathcal{C}| = (\text{N}^\circ \text{ de clases de equivalencia})(\text{tamaño de cada clase}).$$

Pero es fácil ver que hay tantas clases de equivalencia con respecto a $\sim$ como distintas palabras en $\mathcal{B}$, las palabras que queremos contar. Por ende, $7! = |\mathcal{B}|3!$ y concluimos que

$$|\mathcal{B}| = \frac{7!}{3!} = (7)(6)(5)(4) = 840.$$

Una manera alternativa de resolver el problema planteado en el ejercicio anterior es esta: para formar una palabra a partir de las siete fichas en cuestión debemos introducir las letras M, A, N, A, D, A y S en los espacios numerados del 1 al 7:

$$\begin{array}{ccccccccccccc} [& &] & [& &] & [& &] & [& &] & [& &] & [& &] & [& &] \\ & 1 & & & 2 & & & 3 & & & 4 & & & 5 & & & 6 & & & 7 \end{array}$$

(a) Primero introducimos las tres letras A. Para hacer esto debemos elegir tres casillas entre $1, 2, 3, 4, 5, 6, 7$, lo que equivale a elegir un subconjunto del conjunto $\{1, 2, 3, 4, 5, 6, 7\}$ de tamaño 3, y esto lo podemos hacer de $\binom{7}{3}$ formas distintas.

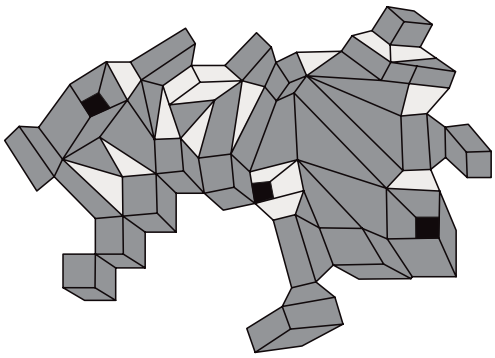
(b) Ahora introducimos las cuatro letras (M, N, D, S) en las cuatro casillas distintas. Para ubicar la M tenemos 4 opciones. Una vez hecho esto, para ubicar la N tenemos 3 opciones. Una vez hecho esto, para ubicar la D tenemos 2 opciones y, una vez hecho esto, para ubicar la S tenemos sólo una opción. Entonces contamos con

$$4! = (4)(3)(2)(1)$$

formas distintas de colocar las letras M, N, D, S.

Concluimos que podemos formar un total de $\binom{7}{3}4! = \frac{7!4!}{3!4!} = \frac{7!}{3!} = 840$ palabras distintas.

Ejercicios



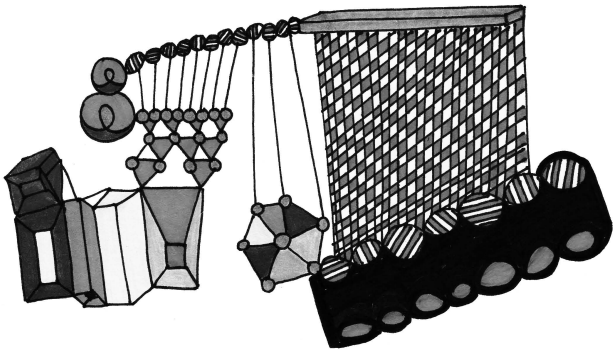
1. Demuestre el Lema 4.91.
2. Calcule el número de palabras distintas de longitud 8 que pueden hacerse utilizando únicamente y los bloques

$$[A], [E], [G], [E], [E], [R], [V], [R].$$

3. Calcule el número de palabras distintas de longitud 8 que pueden hacerse utilizando únicamente los bloques
$$[A],[E],[G],[E],[E],[R],[V],[R],[Z],[K].$$
4. Sean $k, n \in \mathbb{N}^*$. Supongamos que tenemos k cubos negros idénticos y n cubos distintos entre sí de color distinto de negro. Determine el número de torres distintas que podemos construir utilizando los $n+k$ cubos.
5. Se dispone de 4 sombreros blancos, idénticos entre sí y 3 sombreros negros idénticos entre sí. 7 personas se colocarán cada uno un sombrero. ¿De cuántas formas distintas se puede hacer esto?
6. Se tienen 6 piedras preciosas distintas para hacer un collar. ¿Cuántos collares distintos podemos hacer? (En este caso, dos collares M y N se consideran distintos si y sólo si existe al menos una piedra preciosa, cuyo conjunto de dos piedras vecinas en el collar M es distinto del conjunto de sus dos piedras vecinas en el collar N.)
7. Sea $n \in \mathbb{N}^*$. Determine el tamaño del conjunto
$$A = \{\{x, y\} : x, y \in \mathbb{N}, x + y = n\}.$$
8. Se va a partir un palo de longitud 24 en 3 palos de longitudes enteras y todas distintas entre sí. ¿De cuántas formas esencialmente distintas podemos realizar esta tarea?
9. Se dispone de 30 monedas para hacer una compra de bananos, manzanas y peras en un supermercado. Si cada fruta cuesta una moneda y queremos gastar todas las monedas, entonces ¿cuántas compras esencialmente distintas podemos hacer? (Supongamos, además, que el supermercado tiene por lo menos 30 unidades de cada tipo de fruta.)
10. Se dispone de 3 colores distintos para pintar los lados de un hexágono. ¿De cuántas formas esencialmente distintas podemos hacer esta tarea?
11. Se dispone de 3 colores distintos para pintar los lados de un hexágono, de modo que a lados adyacentes se le asignen colores distintos. ¿De cuántas formas esencialmente distintas podemos hacer esta tarea?
12. Se dispone de 5 colores distintos para pintar las 4 caras de una pirámide triangular. ¿De cuántas formas esencialmente distintas podemos hacer esta tarea?
13. Se dispone de 2 colores distintos para pintar las caras de un cubo. ¿De cuántas formas esencialmente distintas podemos hacer esta tarea?

14. Se dispone de 10 colores distintos para pintar las caras de un cubo, de modo que a caras distintas se le asignen colores distintos. ¿De cuántas formas esencialmente distintas podemos hacer esta tarea?
15. Se dispone de 2 colores distintos para pintar las 12 aristas de un cubo, de modo que se le asignen colores distintos a aristas no adyacentes. ¿De cuántas formas esencialmente distintas podemos hacer esta tarea?

Proyecto: Relaciones y matrices booleanas



En este proyecto fijamos un conjunto finito X y a cada relación sobre X le asociamos una matriz cuadrada que codifica toda la información sobre la relación. El proyecto consiste en estudiar cómo las distintas propiedades y operaciones referentes a las relaciones pueden verse como propiedades y operaciones entre sus matrices asociadas.

Matriz

Una *matriz* A de $n \times m$ es un arreglo bidimensional de elementos a_{ij}, $1 \leq i \leq n$, $1 \leq j \leq m$, llamadas sus *entradas*. Cuando nos refiramos a una matriz con una letra mayúscula, nos referiremos a sus entradas i, j con la letra minúscula correspondiente subindexada por i, j.

Dadas las matrices A y B, de $n \times m$, se tiene que $A = B$ si y sólo si para todo i, j con $1 \leq i \leq n$, $1 \leq j \leq m$ se tiene que $a_{ij} = b_{ij}$. Diremos que una matriz es *booleana* si todas sus entradas son unos o ceros. Sea B_n el conjunto de todas las matrices booleanas de $n \times n$.

Sea X un conjunto finito con n elementos, $X = \{x_1, \ldots, x_n\}$ y sea R una relación sobre X. Definimos la matriz A_R como la matriz de $n \times n$ cuya entrada i, j tiene un 1 si $(x_i, x_j) \in R$, y un 0 de lo contrario. Llamaremos a A_R la *matriz booleana asociada a* R. Note que hemos definido implícitamente una función que le asocia un elemento de B_n a cada relación sobre X.

Problemas

1. Demuestre que la función $A : \mathcal{P}(X^2) \to B_n$, la cual le asigna a cada relación R la matriz booleana A_R, es una biyección.
2. Demuestre que R es reflexiva sobre X si y sólo si todas las entradas en la diagonal de A_R son 1.
3. Demuestre que $A_{R^{-1}} = A_R^t$. Es decir, la matriz booleana asociada a la inversa de una relación es la transpuesta de la matriz booleana asociada a la relación. (Dada una matriz A, se define A^t como la matriz cuya entrada i, j es igual a a_{ji}. La matriz A^t es llamada la *transpuesta de A*.)
4. Demuestre que R es simétrica si y sólo si la matriz A_R es simétrica. (Una matriz A es *simétrica* si es igual a su transpuesta, es decir, si $A = A^t$.)
5. Para este ejercicio considere la siguiente definición:

   Definición (conjunción y disyunción). Sobre el conjunto $\{0,1\}$ definimos las operaciones $\vee$ y $\wedge$ así (para $x, y \in \{0,1\}$):

   $$x \vee y := \text{MÁX}(x, y);$$
   $$x \wedge y := \text{MÍN}(x, y).$$

   Es fácil ver que las operaciones $\vee$ y $\wedge$ son asociativas. Dadas las matrices booleanas (esto es, con entradas en $\{0,1\}$) de $n \times n$ A y B, definimos su *disyunción* $A \vee B$ como la matriz booleana C de $n \times n$ cuya entrada i, j está dada por $c_{ij} := a_{ij} \vee b_{ij}$, donde a_{ij} es la entrada i, j de A, y b_{ij} es la entrada i, j de B. De forma análoga definimos la *conjunción* entre A y B, denotada como $A \wedge B$.

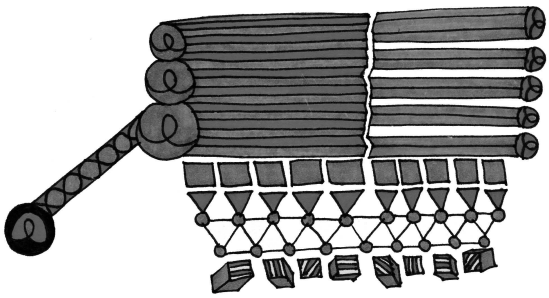
   Demuestre que si R y S son relaciones sobre X, se sigue entonces que $A_{R \cup S} = A_R \vee A_S$ y $A_{R \cap S} = A_R \wedge A_S$.
6. Dadas las matrices booleanas A y B de $n \times n$, definimos su *producto booleano* $A \cdot B$ como la matriz booleana C de $n \times n$ cuya entrada i, j está dada por

   $$c_{ij} := (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \cdots \vee (a_{in} \wedge b_{nj}),$$

   donde a_{ij} es la entrada i, j de A, y b_{ij} es la entrada i, j de B. Demuestre que si R y S son relaciones sobre X, se tiene entonces que $A_{R \circ S} = A_R \cdot A_S$.
7. Dadas dos matrices A y B de $n \times n$, diremos que A es *menor o igual a* B, y lo simbolizamos como $A \leq B$, si y sólo si para todo i, j tales que $1 \leq i \leq n$ y $1 \leq j \leq n$, se tiene que $a_{ij} \leq b_{ij}$. Demuestre que si R y S son relaciones sobre X, entonces $R \subseteq S$ si y sólo si $A_R \leq A_S$.
8. Demuestre que R es una relación transitiva si y sólo si $A_R \cdot A_R \leq A_R$.

9. *Clausuras de una relación*. Demuestre las siguientes afirmaciones:
   (a) $A_{\overline{R}_{\text{REF}}} = A_R \vee \text{ID}_{n\times n}$. ($\text{ID}_{n\times n}$ es la matriz identidad de $n\times n$, cuyas entradas son unos en la diagonal, y ceros en el resto.)
   (b) $A_{\overline{R}_{\text{SIM}}} = A_R \vee A_R^t$.
   (c) $A_{\overline{R}_{\text{TR}}} = A_R \vee (A_R \cdot A_R) \vee \cdots \vee (\underbrace{A_R \cdot A_R \cdots A_R \cdot A_R}_{n \text{ veces}})$.

Lecturas adicionales

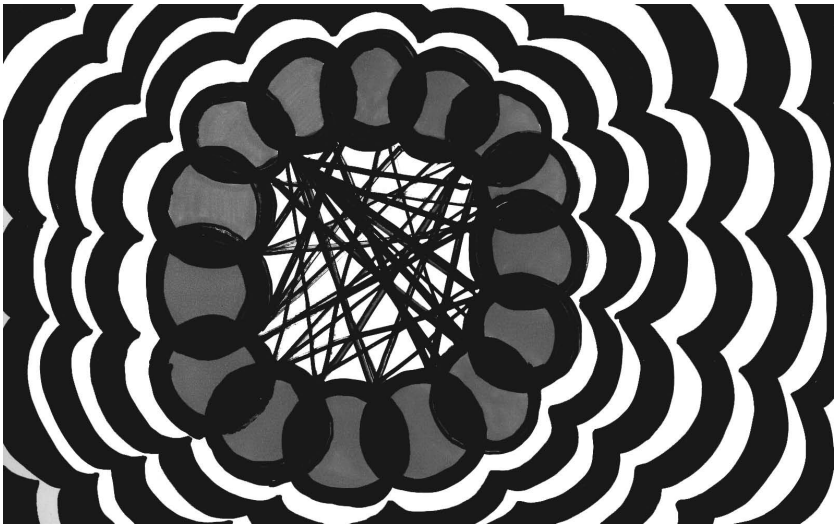


Se recomienda consultar las siguientes lecturas, con miras a profundizar en algunos de los temas tratados en este capítulo:

- Para más información sobre relaciones, consulte [2], § 1.3; [4], § 2.2; [6], § 2.2.
- Para más información sobre órdenes, consulte [4], § 2.5.
- Para más información sobre funciones, consulte [8], §§ 1.6 y 1.7; [2], § 1.3; [4], § 2.3; [6], § 2.4; [11], §§ 20 y 22.
- Para más información sobre relaciones de equivalencia, consulte [8], §§ 1.8 y 1.7, [2], § 1.4; [4], § 2.4; [6], § 2.3; [11], §§ 12 y 13.
- Para más información sobre la construcción de los números enteros y racionales, consulte [5], § 1.5; [4], § 10.1; [2], § 1.8.
- Para más información sobre relaciones y matrices booleanas, consulte [9], c. 7.
- Para más información sobre isomorfismos entre grafos, consulte [6], § 4.5.

CAPÍTULO 5

CARDINALES



Conjuntos cada vez con mayor tamaño...

En este capítulo no nos interesa estudiar la naturaleza y el orden de los elementos de un conjunto, sino únicamente el "tamaño" del conjunto o, dicho de otro modo, la *cantidad* de elementos que tiene. Esto es, nos olvidaremos de las propiedades intrínseca de los elementos del conjunto y de cómo los podemos ordenar, y nos limitaremos a *contarlos*. En el camino obtendremos varios resultados sorprendentes y aparentemente paradójicos, como son los siguientes: (a) existen conjuntos que tienen subconjuntos propios con el mismo tamaño, (b) existen varios tipos de infinitos y (c) no existe un conjunto cuyo tamaño sea mayor o igual al tamaño del resto de los conjuntos.

§ 5.1 Conceptos fundamentales

¿Bajo qué condiciones podemos decir que dos conjuntos X y Y tienen el mismo tamaño? Para responder a esta pregunta, necesitamos una

función f que le asocie a cada elemento de X un elemento en Y, de manera que para todo $y \in Y$ exista un único $x \in X$ tal que $f(x) = y$.

La anterior condición la logran precisamente las biyecciones.

Observación 5.1. $f : X \to Y$ es una biyección si y sólo si para todo $y \in Y$ existe un único $x \in X$ tal que $f(x) = y$.

Para fijar estas ideas, pensemos en el conjunto X de seres vivientes en el universo, el cual podría ser infinito, y en el conjunto Y de todos los planetas del universo. Para responder a la pregunta por si hay tantos seres vivos cuantos planetas, antes que nada hay que establecer si es posible inventar una ley universal (esto es, una función) $f : X \to Y$ que obligue a cada ser vivo x a vivir en un único planeta $f(x) \in Y$, de modo que se cumplan las siguientes condiciones:

(a) que no se manden dos seres distintos a vivir al mismo planeta, porque de lo contrario habría planetas que "contarían" por dos o más seres;

(b) que todo planeta sea habitado por algún ser vivo, porque de lo contrario se podría pensar que *no* alcanzaron los seres vivos para habitar todos los planetas.

Es claro que las condiciones anteriores equivalen a decir que f es una biyección. Esto motiva la siguiente definición:

$|X| = |Y|$: *Relación de equipotencia*

Definición 5.2 (Relación de equipotencia). Dados dos conjuntos X y Y, definimos la *relación de equipotencia* $\sim$ así: $X \sim Y$ si y sólo si existe una biyección $f : X \to Y$. La expresión $X \sim Y$ también se simboliza $|X| = |Y|$ y se lee X *es equipotente a* Y.

Teorema 5.3. La relación de equipotencia es una relación de equivalencia, es decir, una relación reflexiva, simétrica y transitiva.

Prueba.

(a) *Reflexividad*: sea X un conjunto. Sabemos que $\mathrm{ID}_X : X \to X$ es una biyección. Luego $X \sim X$.

(b) *Simetría*: sean X, Y conjuntos. Supongamos que $X \sim Y$. Por ende, existe una biyección $f : X \to Y$. Entonces $f^{-1} : Y \to X$ es una biyección y, por lo tanto, $Y \sim X$.

(c) *Transitividad*: sean X, Y y Z conjuntos. Supongamos que $X \sim Y$ y $Y \sim Z$. Entonces, por definición, existen ciertas funciones biyectivas $f : X \to Y$ y $g : Y \to Z$. Pero entonces $(g \circ f) : X \to Z$ es una biyección. Luego, por definición, $X \sim Z$. ∎

Por convención acordaremos que las siguientes expresiones son equivalentes:

(a) $X \sim Y$;

(b) X y Y son equipotentes;

(c) X y Y son isomorfos como conjuntos;

(d) X y Y tienen el mismo tamaño;

(e) X y Y tienen el mismo cardinal;

(f) $|X| = |Y|$.

El lector podría estar tentado a concluir que $|X|$ significa el tamaño del conjunto X. Por ejemplo, $|\varnothing| = 0$, $|\{1,3,4,6\}| = 4$, etc. Para conjuntos finitos esto no representa dificultad alguna. Sin embargo, debe quedar claro que no hemos definido el objeto *cardinal de* X ($|X|$) para cualquier conjunto, sea finito o infinito. Apenas hemos definido qué significa que dos conjuntos tengan el mismo cardinal.

☞ **Antes de seguir leyendo**

Demuestre que para todo A, $A = \varnothing$ si y sólo si $|A| = |\varnothing|$.

Ejemplo 5.4. Sea $X = \{1,2,3,4,5,6\}$ y $Y = \{0,2,4,6,8,10\}$. La función $f : X \to Y$ dada por $f(i) = 2i - 2$ es en efecto una biyección. Luego $|X| = |Y|$.

Ejemplo 5.5. Los conjuntos $X = \{1,2\}$ y $Y = \{1,3,4\}$ no tienen el mismo cardinal. Es fácil verificar que ninguna función $f : X \to Y$ es sobreyectiva o, dicho de otro modo, que ninguna función $g : Y \to X$ es inyectiva.

Teorema 5.6. Sean A, A', B y B' conjuntos tales que $|A| = |A'|$ y $|B| = |B'|$. Entonces $|A \times B| = |A' \times B'|$.

Prueba. Por hipótesis existen las funciones biyectivas $f_A : A \to A'$ y $f_B : B \to B'$. Debemos verificar que $|A \times B| = |A' \times B'|$, es decir, debemos

demostrar que existe una función biyectiva $f_{A\times B} : A \times B \to A' \times B'$. Para definirla utilizamos las funciones f_A y f_B de la siguiente manera:

$$f_{A\times B} : A \times B \to A' \times B',$$
$$f_{A\times B}((a,b)) = (f_A(a), f_B(b)) \qquad ((a,b) \in A \times B).$$

Verifiquemos que la función que hemos definido es biyectiva:

(a) Inyectividad: sean $(a,b),(c,d) \in A \times B$ y supongamos que

$$f_{A\times B}((a,b)) = f_{A\times B}((c,d)).$$

De esta manera,

$$(f_A(a), f_B(b)) = (f_A(c), f_B(d))$$

y, por lo tanto,

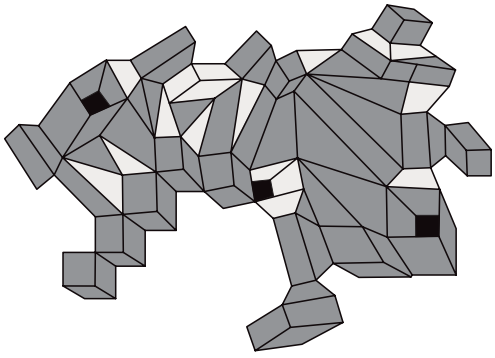
$$f_A(a) = f_A(c) \text{ y } f_B(b) = f_B(d).$$

Por inyectividad de f_A y f_B tenemos que $a = c$ y $b = d$. Entonces $(a,b) = (c,d)$, como queríamos.

(b) Sobreyectividad: sea $(a',b') \in A' \times B'$. Como f_A es sobreyectiva, existe $a \in A$ tal que $f_A(a) = a'$. Como f_B es sobreyectiva, existe $b \in B$ tal que $f_B(b) = b'$. Entonces

$$f_{A\times B}((a,b)) = (f_A(a), f_B(b)) = (a',b').$$ ∎

Ejercicios



1. Demuestre que para todo conjunto A se tiene que $|A| = |A \times \{0\}|$.
2. Demuestre que dados los conjuntos A y B, $|A \times B| = |B \times A|$.
3. Sean $A = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$ y $B = \{2, 4, 6, 8, \ldots\}$. Demuestre que $|A| = |B|$, exhibiendo una biyección entre ambos conjuntos.

4. Dados los conjuntos A, B y C, demuestre que
$$|A \times (B \times C)| = |C \times (A \times B)|.$$
5. Sea $A = \{x \in \mathbb{Q} : 0 < x \leq 1, x = \frac{p}{q} \text{ con } q \text{ un número primo}\}$. Demuestre que $|A| = |\mathbb{N}|$.
6. Sea $A = \{3n + 1 : n \in \mathbb{N}\}$, y $B = \{5n + 5 : n \in \mathbb{N}\}$. Demuestre que $|A| = |B|$, definiendo una biyección explícita entre A y B.
7. Construya una biyección explícita entre el conjunto de los múltiplos enteros de 3 y los múltiplos enteros no negativos de 5.
8. Sea $x \notin A \cup B$. Demuestre la siguiente afirmación:
$$|A| = |B| \leftrightarrow |A \cup \{x\}| = |B \cup \{x\}|.$$
9. Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso (dados A, B y C conjuntos):
   (a) Si $A \subset B$ entonces $|A| \neq |B|$.
   (b) Si $|A| = |B|$ entonces $|A \cap C| = |B \cap C|$.
   (c) Si $|A \cup B| = |A \cup C|$ entonces $|B| = |C|$.
   (d) $|A \times A| \neq |A|$.
10. Sea A un conjunto tal que $|A| = |\mathbb{N}|$. Demuestre que existe un conjunto B tal que $B \subseteq A$ y $|A| = |B| = |A \setminus B|$.
11. Sea A un conjunto tal que $|A| = |\mathbb{N}|$. Demuestre que existen los conjuntos disjuntos entre sí A_1, A_2, A_3, tales que
$$A = A_1 \cup A_2 \cup A_3; \text{ y}$$
$$|A| = |A_1| = |A_2| = |A_3|.$$
12. Suponga que X es un conjunto tal que $|X| = |X \times \{0, 1\}|$. ¿Qué podemos concluir acerca de la cardinalidad de X ?
13. Dado un conjunto X, sea $S(X) = \{\{x\} : x \in X\}$. Demuestre que, dados los conjuntos A y B, $|A| = |B|$ si y sólo si $|S(A)| = |S(B)|$.
14. Dado un conjunto A, sea $D(A)$ el siguiente conjunto:
$$D(A) = \{\{a, b\} : a, b \in A, a \neq b\}.$$
Sean A y B conjuntos tales que $|B| = |B \times B|$. Demuestre que
$$|A| = |B| \text{ si y sólo si } |D(A)| = |D(B)|.$$
15. Sea X un conjunto cualquiera y sea a tal que $a \notin X$. Demuestre que
$$|\mathcal{P}(X)| = |\mathcal{P}(X \cup \{a\}) \setminus \mathcal{P}(X)|.$$

§ 5.2 El Teorema de Cantor-Schröder-Bernstein

A continuación definimos una relación entre conjuntos más débil[1] que la equipotencia:

$|A| \leq |B|$: *Sumersión*

Definición 5.7 (Sumersión). Dados dos conjuntos A y B, definimos la relación *sumersión* así: *A se sumerge en B* si y sólo si existe una función inyectiva $f : A \to B$, lo que simbolizamos $|A| \leq |B|$.

Por definición, diremos que $|X| < |Y|$ si $|X| \leq |Y|$ y no ocurre que $|X| = |Y|$ o, en otras palabras, si existe una función inyectiva $f : X \to Y$, pero no existe una biyección $g : X \to Y$.

> ☞ **Antes de seguir leyendo**
>
> Demuestre las siguientes afirmaciones:
>
> 1. Si $|X| = |Y|$, entonces $|X| \leq |Y|$ y $|Y| \leq |X|$.
> 2. Si $X \subseteq Y$, entonces $|X| \leq |Y|$.
> 3. $|X| \leq |Y|$, si y sólo si existe $C \subseteq Y$ tal que $|X| = |C|$.

Es fácil ver que $|X| \leq |X|$. Para esto, basta tomar como testigo la función inyectiva $\mathrm{ID}_X : X \to X$. Además, si $|X| \leq |Y| \leq |Z|$, entonces $|X| \leq |Z|$ por el Teorema 4.50. De esta manera, la relación $\leq$ es reflexiva y transitiva. Una pregunta natural es la siguiente: si $|A| \leq |B|$ y $|B| \leq |A|$, ¿podemos concluir que $|A| = |B|$? Esta pregunta debe considerarse con cierto cuidado, teniendo en cuenta que el símbolo $\leq$ tiene aquí el significado preciso que ha sido dado en la definición anterior. Un lector desprevenido podría sentirse tentado a concluir que la respuesta a la pregunta anterior es evidentemente afirmativa, dejándose guiar, por ejemplo, por su conocimiento de la antisimetría del orden $\leq$ en los números reales.

Si reformulamos la pregunta anterior haciendo uso de las definiciones, ésta toma la siguiente forma:

Sean X y Y conjuntos. Supongamos que

(a) existe una función inyectiva $f : X \to Y$; y

(b) existe una función inyectiva $g : Y \to X$.

[1] Dadas dos relaciones E_1, E_2 diremos que E_1 es *más débil* que E_2, si y sólo si siempre que dos elementos se relacionen bajo E_2, entonces también se relacionan bajo E_1. Por ejemplo, en los números reales la relación $\leq$ es más débil que la relación $<$.

Entonces, ¿existe necesariamente una función biyectiva $h : X \to Y$? La respuesta a esta pregunta es afirmativa y se conoce como el Teorema de Cantor-Schröder-Bernstein:

Teorema 5.8 (Teorema de Cantor-Schröder-Bernstein, TCSB). Dados X, Y conjuntos, si $|X| \leq |Y|$ y $|Y| \leq |X|$, entonces $|X| = |Y|$.

TCSB: *Teorema de Cantor-Schröder-Bernstein*

Prueba. A continuación demostraremos el teorema en el caso particular en que los dos conjuntos son disjuntos, lo que en principio parecería una pérdida de generalidad. Sin embargo, si adicionalmente demostramos que a partir del resultado particular para conjuntos disjuntos podemos deducir el resultado para cualquier par de conjuntos, entonces habremos demostrado el teorema. En otras palabras, si demostramos que el caso particular implica el caso general, realmente no perdemos generalidad al suponer que X y Y son disjuntos en la demostración del teorema. Resumiendo lo anterior, para establecer el teorema demostraremos dos afirmaciones por separado:

(a) el TCSB es válido para conjuntos disjuntos;

(b) si el TCSB es válido para conjuntos disjuntos, entonces es válido para cualquier par de conjuntos.

Este tipo de razonamiento es común en matemáticas. Para demostrar una afirmación primero "perdemos generalidad" al demostrarla para ciertos casos particulares (en nuestro caso, conjuntos disjuntos) y después "recobramos la generalidad" al demostrar cómo deducir la afirmación en el caso general a partir del caso particular. Ahora sí procedamos a demostrar las dos afirmaciones anteriores; comencemos por la segunda:

(a) Supongamos que el TCSB es verdadero para conjuntos disjuntos y demostrémoslo para conjuntos arbitrarios. Sean X y y tales que $|X| \leq |Y| \leq |X|$. Entonces existen las funciones inyectivas

$$f : X \to Y, \qquad g : Y \to X.$$

Para demostrar que $|X| = |Y|$ debemos encontrar una biyección $h : X \to Y$. Como estamos suponiendo que el teorema es válido si X y Y son disjuntos, aunque éstos no lo sean necesariamente, debemos "volverlos disjuntos" de una manera efectiva. Para esto, sean

$$X' = X \times \{0\}, \qquad Y' = Y \times \{1\}.$$

Es fácil ver que X' y Y' son conjuntos disjuntos y que son además equipotentes a X y Y respectivamente. La función $\alpha : X \to X'$ dada

por $\alpha(x) = (x, 0)$ es una biyección, así como la función $\beta : Y \to Y'$ dada por $\beta(x) = (x, 1)$. Entonces las funciones

$$f' = \beta \circ f \circ \alpha^{-1} : X' \to Y',$$
$$g' = \alpha \circ g \circ \beta^{-1} : Y' \to X'$$

son inyectivas (véase la Figura 5.1), luego $|X'| \leq |Y'| \leq |X'|$. Por ende $|X'| = |Y'|$, por hipótesis, pues $X' \cap Y' = \varnothing$. Pero $|X| = |X'|$ y $|Y| = |Y'|$. Entonces, por la transitividad de la relación equipotencia (Teorema 5.3), concluimos que $|X| = |Y|$, como queríamos.

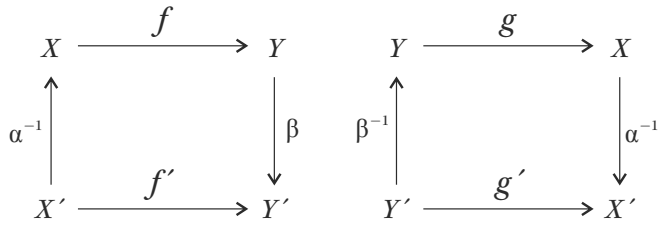


Figura 5.1 : La composición de funciones inyectivas es inyectiva.

(b) Sean X y Y conjuntos disjuntos y sean $f : X \to Y$, $g : Y \to X$ funciones inyectivas. Dados dos elementos a, b, diremos que a es un *ancestro* de b si $f(a) = b$ o $g(a) = b$. La primera observación que hacemos es que todo elemento tiene a lo sumo un ancestro; pues, si a y a' son ancestros de b, entonces $f(a) = b$ o $g(a) = b$, y análogamente $f(a') = b$ o $g(a') = b$. Si $f(a) = b$, concluimos que $b \in Y$. Luego no puede ocurrir que $g(a') = b$ pues de lo contrario $b \in X$, pero X y Y son disjuntos. Así que $f(a') = b$. Pero entonces $f(a) = f(a')$ y como f es inyectiva, $a = a'$. El caso en el cual $g(a) = b$ es análogo.

Ahora, dado un elemento cualquiera $a \in X \cup Y$, una *cadena de ancestros* para a es una tupla de la forma

$$(c_0, c_1, \ldots, c_n),$$

en donde cada c_i es un ancestro de c_{i+1} y $c_n = a$. Además, diremos que n es la *profundidad* de la cadena. Note que el número de elementos de la cadena es igual a $n + 1$. La terminología anterior permite clasificar a los elementos de $X \cup Y$ según sus ancestros. Así, para todo elemento $a \in X \cup Y$, ocurre exactamente uno de los siguientes casos:

(i) a tiene cadenas ancestrales de longitudes arbitrariamente grandes. En este caso diremos que a tiene una profundidad infinita.

(ii) a tiene una única cadena ancestral finita $(c_0, c_1, \cdots, c_{n-1}, a)$, cuyo primer elemento c_0 no tiene ancestros. Es claro que tal cadena es única, ya que cada elemento tiene a lo sumo un ancestro. En este caso diremos que la profundidad de a es igual a n. Por ejemplo, los elementos de profundidad 0 son precisamente aquellos que no tienen ancestros.

Definimos los siguientes conjuntos:

$$X_\infty := \{a \in X : \ a \text{ tiene profundidad infinita}\};$$
$$X_{\text{PAR}} := \{a \in X : \ a \text{ tiene profundidad par}\};$$
$$X_{\text{IMPAR}} := \{a \in X : \ a \text{ tiene profundidad impar}\}.$$

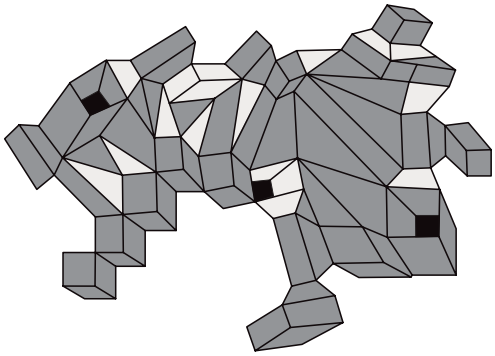
Puede verse a partir de las definiciones anteriores que estos conjuntos son disjuntos y que su unión es exactamente X. Definimos la función $h : X \to Y$ así:

$$h(a) = \begin{cases} f(a) & \text{si } a \in X_{\text{PAR}} \cup X_\infty; \\ g^{-1}(a) & \text{si } a \in X_{\text{IMPAR}}. \end{cases}$$

(Es tarea del lector demostrar que esta función resulta ser una biyección entre X y Y (ejercicio 3).)

Concluimos que $|X| = |Y|$, como queríamos. ∎

Ejercicios



1. Demuestre que si $A \subseteq B$ y $|B| \leq |C|$, entonces $|A| \leq |C|$.
2. Demuestre que si $|A| = |B|$ y $|C| = |D|$ entonces se tiene que $|A| \leq |C|$ si y sólo si $|B| \leq |D|$.

3. Demuestre que la función h que se definió en la prueba del Teorema 5.8 es biyectiva.
4. Sea $n \in \mathbb{N}^*$ y sea A un conjunto (posiblemente infinito). Demuestre que $|\mathcal{P}_n(A)| \leq |A^n|$. (Recuerde que $\mathcal{P}_n(A)$ es la colección de todos los subconjuntos de A con exactamente n elementos y A^n es el conjunto de todas las n-tuplas de elementos de A.)
5. Sea $\sim$ una relación de equivalencia sobre X.
   (a) Demuestre que $|X/\sim| \leq |X|$.
   (b) Demuestre que para todo conjunto C de representantes de $\sim$ se tiene que $|X/\sim| = |C|$.

§ 5.3 Conjuntos finitos

Dado $n \in \mathbb{N}$ definimos los conjuntos A_n recursivamente:

(a) $A_0 := \varnothing$.
(b) $A_{n+1} := A_n \cup \{n\}$.

A_n: Conjunto canónico de n elementos

A_n es llamado *el conjunto canónico de n elementos*. Es fácil ver que para $n > 0$ tenemos que

$$A_n = \{0, \ldots, n-1\}.^2$$

Recordemos que, por definición, un conjunto X tiene 0 elementos si $X = \varnothing$; X tiene $n+1$ elementos si $X \neq \varnothing$; y, para todo $x \in X$, $X \setminus \{x\}$ tiene n elementos.

Lema 5.9. Sea X un conjunto. Para todo $n \in \mathbb{N}$ las siguientes afirmaciones son equivalentes:

(i) X tiene n elementos;
(ii) $|X| = |A_n|$.

Prueba. Hacemos inducción en n:

(a) Caso base ($n = 0$): si X tiene 0 elementos, entonces por definición $X = \varnothing$. Luego, por reflexividad, $|X| = |A_0|$ (véase la parte (c) del *Para antes de seguir leyendo* que precede a la Observación 4.44). Para la otra implicación, si $|X| = |A_0|$, entonces existe una biyección $f : X \to \varnothing$, lo que implica que X debe ser vacío. Luego X tiene 0 elementos.

[2] De hecho, $A_n = n$. Véase el ejercicio 15 de la § 2.2.

(b) Paso inductivo: supongamos que la propiedad es válida para n y demostrémosla para $n+1$:

($\rightarrow$) Si X tiene $n+1$ elementos, entonces $X \neq \varnothing$, y para todo $x \in A$ se tiene que $X \setminus \{x\}$ tiene n elementos. Tomemos $x_0 \in X$, el cual existe, pues X no es vacío. Entonces $X' = X \setminus \{x_0\}$ tiene n elementos, luego por hipótesis de inducción $|X'| = |A_n|$. Sea $f' : X \to A_n$ una función biyectiva. Definimos $f : X \to A_{n+1}$ así:

$$f(x) = \begin{cases} f'(x) \text{ si } x \neq x_0; \\ n \text{ si } x = x_0. \end{cases}$$

Es fácil ver que f es biyectiva. Luego $|X| = |A_{n+1}|$.

($\leftarrow$) Supongamos que $|X| = |A_{n+1}|$. Entonces existe una función biyectiva $f : X \to A_{n+1}$. Queremos ver que X tiene $n+1$ elementos. La existencia de f garantiza que $X \neq \varnothing$, pues $A_{n+1} \neq \varnothing$. Ahora, sea $x_0 \in X$ y sea f' la restricción de f a $X' = X \setminus \{x_0\}$. Si $f(x_0) = n$, entonces $f' : X' \to A_n$ es una biyección. Si este no es el caso, entonces existe $y \in X'$ tal que $f'(y) = n$ (véase la Figura 5.2). Definimos $g : X' \to A_n$ así:

$$g(x) = \begin{cases} f(x) \text{ si } x \in X'; \\ f(x_0) \text{ si } x \neq y. \end{cases}$$

Dejamos al lector la tarea de verificar que g es una biyección. En cualquier caso hemos demostrado que existe una biyección entre X' y A_n y, por ende, $|X'| = |A_n|$. Entonces, por hipótesis de inducción, X' tiene n elementos.

Concluimos que $X \neq \varnothing$ y, para todo $x_0 \in X$, $X' = X \setminus \{x_0\}$ tiene n elementos; luego X tiene $n+1$ elementos. ∎

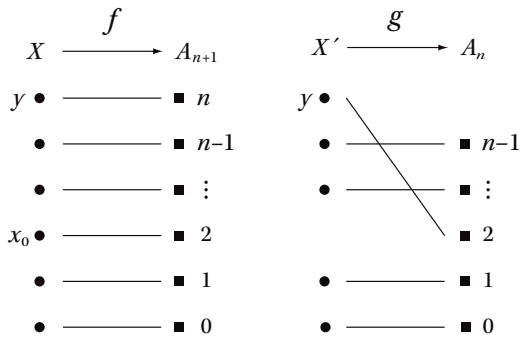


Figura 5.2: Lema 5.9. Se ilustra el caso en que $f(x_0) \neq n$.

Gracias al lema anterior, podemos reformular la Definición 2.25 así:

Conjunto finito

Definición 5.10 (Conjunto finito, reformulación). Un conjunto X es *finito* si existe $n \in \mathbb{N}$ tal que $|X| = |A_n|$.

Por la reflexividad de la relación de equipotencia, todo A_n es finito. Algunos conjuntos finitos son $\{1, 2, 4\}$, $\{a, 3, 0, 10, 11\}$ y $\{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$. Además, $\varnothing$ es finito pues es equipotente y, en efecto, igual a A_0.

Si A es un conjunto finito no vacío, entonces existe un número natural positivo n y una biyección $a : A_n \to A$, de manera que si definimos $a_i = a(i) \in A$ para $i = 0, \ldots, n$, podemos decir, puesto que a es sobreyectiva, que $A = \text{IMG}(a) = \{a_0, \ldots, a_n\}$. Esto justifica que todo conjunto finito distinto de vacío A pueda escribirse en la forma $A = \{a_0, \ldots a_n\}$.

Si $|A| = |A_n|$ con $n \in \mathbb{N}$, entonces por el Lema 5.9, *A tiene n elementos*. A este hecho lo abreviaremos así: $|A| = n$. Puede verse que si A es un conjunto finito, existe un único $n \in \mathbb{N}$ tal que $|A| = |A_n|$ (véase el ejercicio 4). Por ejemplo, si $A = \{3, 6, 7\}$, entonces es fácil ver que $|A| = |A_3|$ y, por tanto, A tiene 3 elementos. El conjunto vacío tiene 0 elementos.

Las siguientes son propiedades esenciales de los conjuntos finitos que consideramos evidentes intuitivamente, aunque en rigor deben ser demostradas.

Teorema 5.11. Las siguientes propiedades son siempre verdaderas:

(a) la unión de dos conjuntos finitos es un conjunto finito;

(b) si A es finito y para todo $a \in A$, a es un conjunto finito, entonces $\bigcup A$ es un conjunto finito;

(c) todo subconjunto de un conjunto finito es finito;

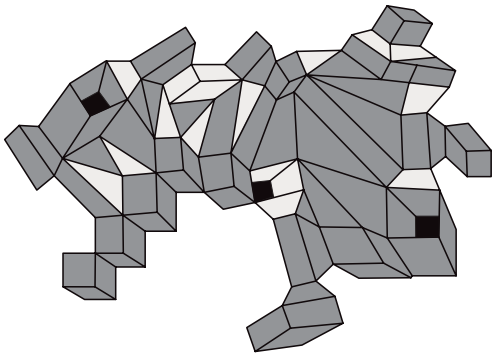
(d) si X es finito y Y está contenido propiamente en X, entonces se tiene que $|Y| < |X|$.

(e) $\mathbb{N}$ no es finito.

Prueba. Las demostraciones de las propiedades (a), (b), (c) y (d) se hacen por inducción matemática, y se dejan al lector (ejercicio 5). La parte (e) ya ha sido demostrada (Corolario 2.27). ∎

En especial, cabe destacar la propiedad (d), que *no* será válida en general para conjunto infinitos: *los conjuntos infinitos tienen subconjuntos propios del mismo cardinal.*

Ejercicios



1. Demuestre que si A y B son conjuntos finitos, entonces $A \cup B$ es finito. (*Ayuda*: utilice inducción en n, en donde $|A| = |n|$.)
2. Demuestre que para todo conjunto no vacío X se tiene que X tiene $n+1$ elementos ($n \in \mathbb{N}$), si y sólo si existe $x \in X$ tal que el conjunto $X \setminus \{x\}$ tiene n elementos. (*Ayuda*: consulte la definición recursiva de "tener n elementos", Definición 2.24. Haga inducción en n.)
3. Demuestre que para todo conjunto A, A es infinito si y sólo si $\mathcal{P}(A)$ es infinito.
4. Demuestre que para todo conjunto finito X existe un único $n \in \mathbb{N}$ tal que $|X| = |A_n|$. (*Ayuda*: demuestre por inducción en n que si $|X| = |A_n|$ entonces para todo $m \in \mathbb{N}$, si $|X| = |A_n|$ entonces $n = m$.)
5. Demuestre las siguientes afirmaciones:
   (a) Si A es finito y para todo $a \in A$ a es un conjunto finito, entonces $\bigcup A$ es un conjunto finito.
   (b) Todo subconjunto de un conjunto finito es finito.
   (c) Si X es finito y $Y \subset X$, entonces $|Y| < |X|$.

§ 5.4 Conjuntos enumerables

Conjunto enumerable

Conjunto a lo sumo enumerable

Definición 5.12. Sea A un conjunto. Diremos que A es *enumerable* si y sólo si $|A| = |\mathbb{N}|$. Además, diremos que A es *a lo sumo enumerable* si y sólo si A es finito o enumerable.

Así, un conjunto A es enumerable si existe una biyección $a : \mathbb{N} \to A$, de modo que $A = \{a_0, a_1, a_2, \dots\}$, donde $a_n = a(n)$.

Ejemplo 5.13. El conjunto $2\mathbb{N} = \{2n : n \in \mathbb{N}\}$ es enumerable, ya que la función $f : \mathbb{N} \to 2\mathbb{N}$ definida por $f(n) = 2n$ es una biyección.

☞ **Antes de seguir leyendo**

Demuestre que $\mathbb{Z}^-$ es un conjunto enumerable.

Teorema 5.14. Si A y B son conjuntos enumerables, entonces existe una biyección $f : A \to B$, esto es, A y B son equipotentes.

Prueba. Es una consecuencia directa del Teorema 5.3. ∎

Lema 5.15. Sea $A \subseteq \mathbb{N}$ un conjunto con la siguiente propiedad:

$$\text{Para todo } x \in \mathbb{N} \text{ existe } m \in A \text{ tal que } m > x. \qquad (*)$$

Entonces, A es un conjunto enumerable.

Prueba. Definimos la función $f : \mathbb{N} \to A$ recursivamente así:

(a) $f(0) = \text{MÍN}(A)$. Note que $\text{MÍN}(A)$ existe por el PBO, más el hecho de que A no puede ser vacío.

(b) $f(n+1) = \text{MÍN}(B)$, en donde $B = \{m \in A : m > f(n)\}$. Note que B es no vacío por la propiedad (*).

Es fácil verificar por inducción que f es una función inyectiva. De hecho, f es una función *estrictamente creciente* (véase el ejercicio 9 de la § 4.3). Veamos que $\text{IMG}(f) = A$:

(⊆) Por definición de f, para todo $n \in \mathbb{N}$ se tiene que $f(n) \in A$.

(⊇) Supongamos —por contradicción— que $\text{IMG}(f) \not\supseteq A$. Sea entonces $b = \text{MÍN}(A \setminus \text{IMG}(f))$. Dado que $\text{MÍN}(A) \in \text{IMG}(f)$, tenemos que $b \neq f(0)$. Entonces el conjunto

$$\{x \in \text{IMG}(f) : x < b\}$$

tiene un elemento máximo de la forma $f(n)$, con $n \in \mathbb{N}$. Sea

$$B = \{m \in A : m > f(n)\}.$$

Es fácil verificar que $b = \text{MÍN}(B)$. Entonces, por definición de f, tenemos que $b = f(n+1)$, lo cual es una contradicción, ya que $b \notin \text{IMG}(f)$. Concluimos que $\text{IMG}(f) \supseteq A$.

Por ende, $f : \mathbb{N} \to A$ es una biyección, luego $|A| = |\mathbb{N}|$. ∎

Como se habrá observado, el argumento en la demostración del lema anterior ya fue utilizado en la demostración de la Observación 3.25.

Teorema 5.16. Dado un conjunto A, A es a lo sumo enumerable si y sólo si $|A| \leq |\mathbb{N}|$.

Prueba. Utilizamos el método de doble implicación:

($\rightarrow$) Supongamos que A es a lo sumo enumerable. Hay dos casos:

(i) A es finito: en este caso existe $n \in \mathbb{N}$ tal que $|A| = |A_n|$. Dado que $|A_n| \leq |\mathbb{N}|$, se sigue que $|A| \leq |\mathbb{N}|$.

(ii) A es enumerable: en este caso $|A| = |\mathbb{N}|$. Luego, en particular, $|A| \leq |\mathbb{N}|$.

En cualquier caso concluimos que $|A| \leq |\mathbb{N}|$.

($\leftarrow$) Supongamos que $|A| \leq |\mathbb{N}|$. Entonces existe una función inyectiva $f : A \to \mathbb{N}$. Hay dos casos:

(i) Existe $n \in \mathbb{N}$ tal que $\text{IMG}(f) \subseteq \{0, 1, \ldots, n\}$. En este caso $\text{IMG}(f)$ es un conjunto finito, por el Teorema 5.11 y el hecho de que $\{0, 1, \ldots, n\} = A_{n+1}$ es finito. Pero claramente $|A| = |\text{IMG}(f)|$ y por ende, A es un conjunto finito. Luego A es a lo sumo enumerable.

(ii) No se da el caso (i), esto es, para todo $n \in \mathbb{N}$ existe m tal que $m > n$ y $m \in \text{IMG}(f)$. Entonces por el Lema 5.15 se tiene que $|\text{IMG}(f)| = |\mathbb{N}|$, pero como f es inyectiva se tiene que $|A| = |\text{IMG}(f)|$. Luego, por el Teorema 5.3, A es un conjunto enumerable y en particular, es a lo sumo enumerable.

En cualquier caso concluimos que A es un conjunto a lo sumo enumerable, como queríamos demostrar. ∎

Una aplicación del anterior teorema es la siguiente:

Corolario 5.17. Los subconjuntos de conjuntos a lo sumo enumerables son a lo sumo enumerables.

Prueba. Sea $A \subseteq B$, con B un conjunto a lo sumo enumerable. Como $A \subseteq B$ tenemos que $|A| \leq |B|$, y como B es a lo sumo enumerable, por el Teorema 5.16, $|B| \leq |\mathbb{N}|$. Por transitividad de la relación de sumersión, concluimos que $|A| \leq |\mathbb{N}|$, lo que implica, de nuevo por el Teorema 5.16, que A es a lo sumo enumerable. ∎

Ejemplo 5.18. Sea $A = \mathbb{N} \setminus \{n_0\}$, donde n_0 es algún número natural. Entonces A es un conjunto enumerable. Para ver esto, sea $f : \mathbb{N} \to A$ la siguiente función:

$$f(n) = \begin{cases} n & \text{si } n < n_0; \\ n+1 & \text{si } n \geq n_0. \end{cases}$$

Por el Lema 4.57, concluimos que f es una función inyectiva y, además,

$$\text{IMG}(f) = \{0, \ldots, n_0 - 1\} \cup \{n_0 + 1, n_0 + 2, \ldots\} = A.$$

Así, $|A| = |\mathbb{N}|$.

Podemos generalizar de manera natural el ejemplo anterior:

Lema 5.19. Si A es un enumerable y $x \in A$, entonces $A' = A \setminus \{x\}$ también es enumerable.

Prueba. Sea $A = \{a_n : n \in \mathbb{N}\}$, donde $n \neq m$ implica $a_n \neq a_m$. Como $x \in A$, sea n_0 tal que $x = a_{n_0}$. La función $f : \mathbb{N} \setminus \{n_0\} \to A'$ dada por $n \mapsto a_n$ es una biyección, por lo que $|A'| = |\mathbb{N} \setminus \{n_0\}| = |\mathbb{N}|$ (esto lo garantiza el ejemplo 5.18). Por transitividad concluimos que $|A'| = |\mathbb{N}|$, esto es, A' es enumerable. ∎

El ejemplo 5.18 es un caso especial del siguiente hecho: si a un conjunto enumerable le quitamos un número finito de elementos, el conjunto resultante sigue siendo enumerable.

Teorema 5.20. Sea A un conjunto enumerable y $B = \{x_1, \ldots, x_n\} \subseteq A$ un conjunto de n elementos ($n \in \mathbb{N}$). Entonces $A' = A \setminus B$ es enumerable.

Prueba. Demostramos el resultado mediante inducción en n.

(a) Caso base ($n = 0$). Entonces $B = \varnothing$ y el resultado es evidente.

(b) Paso inductivo: supongamos que el resultado se tiene para n y sea $B = \{x_1, \ldots, x_n, x_{n+1}\}$. Por hipótesis inductiva, $A \setminus \{x_1, \ldots, x_n\}$ es enumerable; luego, por el Lema 5.19, se tiene que

$$(A \setminus \{x_1, \ldots, x_n\}) \setminus \{x_{n+1}\} = A \setminus B$$

es un conjunto enumerable. ∎

☞ **Antes de seguir leyendo**

Para cada una de las siguientes afirmaciones, determine si es verdadera o falsa. Justifique con una demostración o un contraejemplo, según sea el caso:

1. Si A es enumerable y B es finito, entonces $A \cup B$ es enumerable.
2. Si $A \subseteq \mathbb{N}$ y A es enumerable, entonces $A^c = \mathbb{N} \setminus A$ es finito.

Ahora estudiaremos el cardinal del conjunto $\mathbb{Z}$ de los números enteros. Podría pensarse de forma algo inocente que este conjunto es "el doble" de grande que $\mathbb{N}$, ya que el primer conjunto puede ser imaginado como la unión de dos copias de los naturales, salvo el 0, que sólo estaría en alguna de las copias. Esto es,

$$\mathbb{Z} = \{-1, -2, -3, \dots\} \cup \{0, 1, 2, \dots\}.$$

Sin embargo, si examinamos más detenidamente la cuestión, resulta que $\mathbb{Z}$ y $\mathbb{N}$ son equipotentes, pues existe una forma de emparejar todos los elementos de ambos conjuntos, como lo muestra la siguiente tabla:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	…
0	−1	1	−2	2	−3	3	−4	4	−5	5	−6	6	−7	…

Teorema 5.21. El conjunto $\mathbb{Z}$ es enumerable.

Prueba. Sea $f : \mathbb{N} \to \mathbb{Z}$ la función definida así: dado $n \in \mathbb{N}$, por el Algoritmo de la División existen únicos $q, r \in \mathbb{Z}$ tales que $n = 2q + r$ y, además, $0 \leq r < 2$. Sea $f(n) = (-1)^r(q + r) \in \mathbb{Z}$. Veamos que la función $f : \mathbb{N} \to \mathbb{Z}$ es biyectiva:

(a) Inyectividad: sean $n, n' \in \mathbb{N}$ tales que $f(n) = f(n')$. Sean q, r, q', r' enteros tales que $n = 2q + r$ y $n' = 2q' + r'$ con $0 \leq r, r' < 2$. Tenemos que $q \geq 0$ o, de lo contrario, se tendría que $n < 0$. Análogamente $q' \geq 0$. En conclusión, $r, r', q, q' \geq 0$. Como $f(n) = f(n')$, entonces

$$(-1)^r(q + r) = (-1)^{r'}(q' + r').$$

Si se tuviera que $r \neq r'$, entonces una de las expresiones en la anterior ecuación sería negativa y la otra sería positiva o 0, lo cual es absurdo. Así, $r = r'$. Dividiendo la ecuación anterior a ambos lados por $(-1)^r$ obtenemos que $q + r = q' + r'$, luego $q = q'$, y

$$n = 2q + r = 2q' + r' = n',$$

como queríamos demostrar.

(b) Sobreyectividad: sea $a \in \mathbb{Z}$ cualquiera. Hay dos casos:

(i) $a \geq 0$: sea $n = 2a + 0 \in \mathbb{N}$. Entonces, por definición de f, tenemos que $f(n) = (-1)^0(a+0) = 1(a) = a$.

(ii) $a < 0$: en este caso $-a - 1 \in \mathbb{N}$. Sea $n = 2(-a-1)+1 \in \mathbb{N}$. Luego $f(n) = (-1)^1(-a-1+1) = (-1)(-a) = a$, por definición de f.

En ambos casos vemos que existe $n \in \mathbb{N}$ tal que $f(n) = a$. Por lo tanto, f es sobreyectiva.

Concluimos que $|\mathbb{N}| = |\mathbb{Z}|$, luego $\mathbb{Z}$ es enumerable. ∎

Corolario 5.22. La unión de dos conjuntos enumerables es enumerable. Esto es, si $|A| = |\mathbb{N}|$ y $|B| = |\mathbb{N}|$ entonces $|A \cup B| = |\mathbb{N}|$.

Prueba. Como A es enumerable, existe una biyección $f : \mathbb{N} \to A$. Como B es enumerable y el conjunto $\mathbb{Z}^-$ también lo es, entonces, por el Teorema 5.14, existe una biyección $g : B \to \mathbb{Z}^-$. A partir de f y g definimos la función $h : A \cup B \to \mathbb{Z}$ por casos:

$$h(x) = \begin{cases} f(x) & \text{si } x \in A \setminus B; \\ g(x) & \text{si } x \in B. \end{cases}$$

Gracias al Lema 4.57 es fácil ver que h es una función inyectiva y, por ende, $|A \cup B| \leq |\mathbb{Z}|$. Como $A \subseteq A \cup B$, entonces $|A| \leq |A \cup B|$. En resumen tenemos:

$$|\mathbb{N}| = |A| \leq |A \cup B| \leq |\mathbb{Z}| = |\mathbb{N}|.$$

Por el TCSB tenemos finalmente que $|A \cup B| = |\mathbb{N}|$. ∎

Teorema 5.23. El conjunto $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ es enumerable.

Prueba. Nuestra meta consiste en encontrar una manera de "enumerar" todas las parejas $(n, m) \in \mathbb{N}^2$. Antes de ello, para facilitar las cosas, notemos que el conjunto $\mathbb{N} \times \mathbb{N}$ puede verse como la unión de sus "diagonales finitas" D_n, como lo indica la Figura 5.3. Para todo $n \in \mathbb{N}$, el conjunto D_n, definido como

$$D_n = \{(k,l) \in \mathbb{N}^2 : k + l = n\} = \{(0,n), (1,n-1), \ldots, (n,0)\},$$

tiene $n+1$ elementos y es claro que $\bigcup_{n \in \mathbb{N}} D_n = \mathbb{N}^2$. La anterior descripción da una idea para enumerar todas las parejas de números naturales: primero enumerar la pareja $(0,0)$ de D_0; después las dos parejas de D_1, que son $(0,1)$ y $(1,0)$; a continuación las tres parejas de D_2, que son $(0,2), (1,1)$ y $(2,0)$, etc.

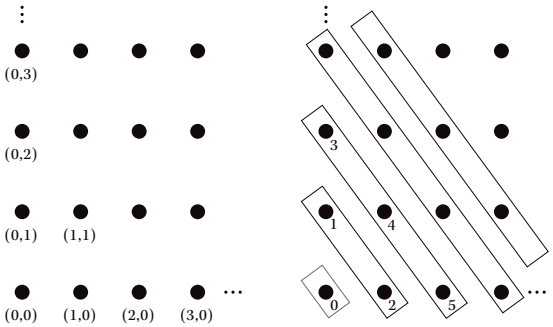


Figura 5.3 : Una de muchas maneras de enumerar el conjunto $\mathbb{N}^2$.

Más precisamente, si $(k,l) \in \mathbb{N}^2$ y $k+l = n$, entonces $(k,l) \in D_n$, así que en la enumeración que proponemos ya habremos enumerado todos los elementos de las diagonales anteriores $D_0,\ldots,D_{n-1}$ y, además, a los k elementos que "preceden" a (k,l) en la diagonal D_n, es decir: $(0,n),(1,n-1),\ldots,(k-1,l+1)$. En otras palabras, suponemos que ya hemos enumerado un total de

$$|D_0| + |D_1| + \cdots + |D_{n-1}| + k = 1 + 2 + \cdots + n + k = (n+1)n/2 + k$$

elementos. Luego (k,l) será el $((n+1)n/2 + k + 1)$-ésimo elemento en el orden que proponemos. Con el fin de formalizar el análisis anterior, definimos la función $f : \mathbb{N}^2 \to \mathbb{N}$ así:

$$f((k,l)) = (k+l+1)(k+l)/2 + k.$$

Por el razonamiento anterior, f es una biyección entre $\mathbb{N}^2$ y $\mathbb{N}$. ∎

Sea f la función definida en la demostración del teorema anterior. Por ejemplo,

$$f((0,0)) = (0+0+1)(0+0)/2 + 0 = 0;$$
$$f((0,1)) = (0+1+1)(0+1)/2 + 0 = 1;$$
$$f((4,4)) = (4+4+1)(4+4)/2 + 4 = 40.$$

En el ejercicio 11 le pedimos al lector demostrar rigurosamente que la función f es una biyección.

Corolario 5.24. Si A y B son conjuntos enumerables, entonces $A \times B$ también lo es.

Prueba. Como $|A| = |B| = |\mathbb{N}|$, entonces por el Teorema 5.6 tenemos que

$$|A \times B| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|.$$ ∎

Corolario 5.25. $\mathbb{Q}$ es un conjunto enumerable.

Prueba. Como $\mathbb{N} \subseteq \mathbb{Q}$, entonces $|\mathbb{N}| \leq |\mathbb{Q}|$. Ahora, sea $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ la siguiente función: dado $r \in \mathbb{Q}$, es fácil ver que r se escribe de manera única como $\frac{p}{q}$, con $q > 0$ y p y q primos relativos (considere el ejercicio 10 de la § 3.2). Sea $f(r)$ dada por

$$f\left(\frac{p}{q}\right) = (p, q) \in \mathbb{Z} \times \mathbb{N}.$$

Es fácil ver que esta función es inyectiva, de modo que:

$$|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}| = |\mathbb{N}|.$$

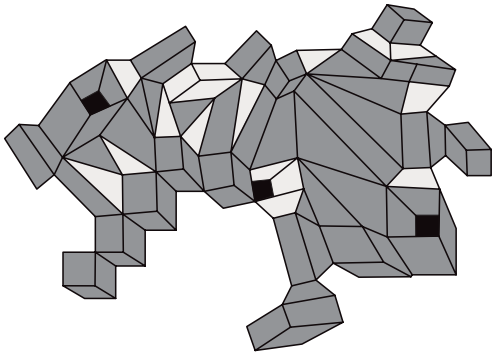
La igualdad vale por el Corolario 5.24. Por el TCSB, $|\mathbb{Q}| = |\mathbb{N}|$. ∎

Concluimos esta sección con un listado de algunos conjuntos enumerables importantes, a modo de resumen:

Teorema 5.26. Sea $n \in \mathbb{N}^*$. Los siguientes conjuntos son enumerables:

(a) $\mathbb{N}$,
(b) $\mathbb{N}^{\geq n} = \{k \in \mathbb{N} : k \geq n\}$,
(c) $\mathbb{Z}$,
(d) $\mathbb{Z}^{\leq n} = \{k \in \mathbb{Z} : k \leq n\}$,
(e) $\mathbb{Q}$,
(f) $n\mathbb{N} = \{kn : k \in \mathbb{N}\}$,
(g) $\mathbb{N}^n$,
(h) $\mathbb{Z}^n$,
(i) $\mathbb{Q}^n$,
(j) el conjunto de los números primos,
(k) cualquier subconjunto infinito de un conjunto enumerable.

Ejercicios



1. Demuestre que cada uno de los siguientes conjuntos es enumerable, definiendo una biyección explícita entre él y $\mathbb{N}$.
   (a) $\mathbb{N}^*$.
   (b) $\{1/n : n \in \mathbb{N}\}$.
   (c) $\{n \in \mathbb{N} : n \text{ no es un número primo}\}$.
   (d) $\{n + \frac{m}{10} : n, m \in \mathbb{N}\}$.
   (e) $\{n + \frac{m}{10} + \frac{k}{100} : n, m, k \in \mathbb{N}\}$.
   (f) $\{z \in \mathbb{Z} : |z| > 6\}$.
   (g) $\mathbb{N}^{>5}$.
2. Demuestre que si $A \subseteq B$, A es infinito y B es enumerable, entonces A es enumerable.
3. Sea $B = \{q \in \mathbb{Q} : 0 \leq q \leq 1\}$. Demuestre que B es enumerable.
4. Sea $n \in \mathbb{N}$, con $n > 1$. Demuestre que para todo $P \in \mathbb{Z}_n$, P es enumerable.
5. Demuestre que si X es un conjunto enumerable entonces $X \cup \{x_0\}$ es un conjunto enumerable (donde x_0 es un elemento cualquiera).
6. Demuestre que para todo $n \in \mathbb{N}^*$, si $X_1, X_2, \ldots, X_n$ son conjuntos enumerables, entonces $X = X_1 \cup X_2 \cup \cdots \cup X_n$ es enumerable.
7. Sean X un conjunto a lo sumo enumerable y Y un conjunto enumerable. Demuestre que $|X| \leq |Y|$.
8. Sean X un conjunto enumerable y $S \subseteq X$. Demuestre que S es enumerable o $S^c = X \setminus S$ es enumerable.
9. Sea $X = \bigcup_{n \in \mathbb{N}^*} \mathbb{N}^n$. Demuestre que X es enumerable.

10. Sea X un conjunto. Demuestre que las siguientes afirmaciones son equivalentes:
    (a) X es infinito.
    (b) Existe a tal que $a \notin X$ y $|X \cup \{a\}| = |X|$.
    (c) Existe a tal que $a \in X$ y $|X \setminus \{a\}| = |X|$.
    (d) Existe Y tal que $Y \subset X$ y $|X| = |Y|$.
11. Demuestre que la función f definida en el Teorema 5.23 es una biyección.
12. Demuestre que $\mathcal{P}_{\text{FIN}}(\mathbb{N})$, la colección de todos los subconjuntos finitos de $\mathbb{N}$, es un conjunto enumerable.
13. Demuestre que si X es un conjunto enumerable, entonces X es de la forma $X = \bigcup_{n\in\mathbb{N}} X_n$, en donde X_n es un conjunto enumerable y $X_n \cap X_m = \varnothing$ para $n < m$. En otras palabras, demuestre que todo conjunto enumerable puede partirse en un número enumerable de conjuntos enumerables. (*Ayuda*: considere primero el caso en el cual $X = \mathbb{N}$. Piense en conjuntos formados por potencias positivas de números primos.)
14. Sea X un conjunto enumerable. Demuestre que si $\sim$ es una relación de equivalencia sobre X tal que, para todo $a \in X$, $[a]$ es finito, entonces $X/\sim$ es enumerable.

§ 5.5 Conjuntos infinitos no enumerables

Sea A un conjunto cualquiera. Ocurre entonces exactamente alguno de los siguientes tres casos:

(i) A es finito, es decir, existe $n \in \mathbb{N}$ tal que $|A| = |n|$.

(ii) A es enumerable, es decir, $|A| = |\mathbb{N}|$.

(iii) No se dan ni el caso (i) ni el (ii), es decir, A no es finito y A no es enumerable.

En esta sección estudiaremos los conjuntos que cumplen con la condición (iii), esto es, los conjuntos infinitos no enumerables. Puede verse que estos son precisamente aquellos conjuntos A tales que $|\mathbb{N}| < |A|$. Coloquialmente hablando, un conjunto infinito no enumerable tiene un tamaño infinito "más grande" que el infinito del conjunto de los números naturales.

☞ **Antes de seguir leyendo**

Sea A un conjunto cualquiera. Demuestre que las siguientes condiciones son equivalentes:

1. A es infinito no enumerable.
2. Para todo $B \supseteq A$, B es no enumerable.
3. Existe $g : \mathbb{N} \to A$ inyectiva, pero no existe ninguna $f : \mathbb{N} \to A$ sobreyectiva. En particular, $|\mathbb{N}| < |A|$.

¿Existen conjuntos infinitos no enumerables? Esto es, ¿existen conjuntos A que *no* cumplan con que $|A| \leq |\mathbb{N}|$? La respuesta es afirmativa. Más aun, muchos conjuntos familiares son de esta naturaleza como, por ejemplo, el conjunto potencia de $\mathbb{N}$.

Teorema 5.27. $\mathcal{P}(\mathbb{N})$ es un conjunto infinito no enumerable.

Prueba. Para demostrar que $\mathcal{P}(\mathbb{N})$ no es enumerable, basta demostrar que ninguna función $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ es biyectiva. Supongamos por contradicción que existe una función biyectiva $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$. Para todo $n \in \mathbb{N}$, $f(n)$ es un conjunto de números naturales. Entonces, o bien $n \in f(n)$, o bien $n \notin f(n)$. Siendo esto así, consideremos el conjunto

$$S = \{n \in \mathbb{N} : n \notin f(n)\}.$$

Como $S \in \mathcal{P}(\mathbb{N})$ y f es sobreyectiva, existe $n_0 \in \mathbb{N}$ tal que $S = f(n_0)$. Ahora nos preguntamos: ¿pertenece n_0 a S? Si este es el caso, entonces por definición de este conjunto, $n_0 \notin f(n_0)$, lo cual es una contradicción. Entonces $n_0 \notin f(n_0) = S$. Pero entonces por definición de S, $n_0 \in f(n_0)$, lo cual es también una contradicción. En cualquier caso llegamos a algo absurdo (compárese con la Paradoja de Russell, § 1.2, arriba). Concluimos que la función f no puede ser una biyección y por ende, que $\mathcal{P}(\mathbb{N})$ es un conjunto infinito no enumerable. ∎

Hemos probado realmente algo un poco más fuerte: *no existen* funciones sobreyectivas $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$.

Como el lector notará, en la demostración anterior no hemos utilizado en absoluto las propiedades estructurales (aritmética y orden) de la estructura de los números naturales. Cantor descubrió un fenómeno general notable: *todo conjunto es estrictamente más pequeño que su conjunto de partes*.[3]

[3] Esto sucede inclusive con el conjunto vacío, pues $\mathcal{P}(\varnothing)$ contiene un elemento.

Teorema de Cantor

Teorema 5.28 (Teorema de Cantor).[4] Para todo conjunto A,

$$|A| < |\mathcal{P}(A)|.$$

Prueba. La función $g : A \to \mathcal{P}(A)$ dada por $g(x) = \{x\}$ es inyectiva. Esto demuestra que $|A| \leq |\mathcal{P}(A)|$. Si imitamos la prueba del Teorema 5.27, podemos convencernos de que no existen sobreyecciones $f : A \to \mathcal{P}(A)$. Así, en particular, no existen biyecciones $f : A \to \mathcal{P}(A)$. Lo anterior implica que $|A| < |\mathcal{P}(A)|$, por definición (véanse los comentarios después de la Definición 5.7). ∎

Corolario 5.29. No existe un conjunto de tamaño máximo o maximal; en otras palabras, para todo conjunto A existe un conjunto B tal que $|A| < |B|$.

El cardinal del conjunto de los números reales

Un asunto interesante consiste en estudiar el cardinal de $\mathbb{R}$, el conjunto de los números reales. Para esto, note que un número real puede verse como un número de la forma $z + d$, en donde $z \in \mathbb{Z}$ y $0 \leq d < 1$. Entonces d tendrá una representación decimal de la forma

$$d = 0, d_0 d_1 d_2 d_3 \ldots,$$

donde cada d_i es un número natural entre 0 y 9. Por ejemplo, $\pi = 3 + d$, en donde $d = 0,141592\ldots$ Notemos que d puede verse como una tupla infinita de ciertos números naturales. En este caso, d puede verse como la tupla infinita $(1, 4, 1, 5, \ldots)$. Esto da un indicio de cómo aproximarse al estudio del cardinal de $\mathbb{R}$: estudiar el tamaño de ciertos conjuntos de tuplas infinitas. En el siguiente lema hacemos esto en el caso de tuplas infinitas de ceros y unos:

Lema 5.30. Sea $2^{\mathbb{N}} = \{f : f : \mathbb{N} \to \{0, 1\}\}$. Entonces $|2^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$.

Prueba. Podemos ver a $2^{\mathbb{N}}$ como el conjunto de todas las tuplas infinitas de ceros y unos, donde, para todo $f \in 2^{\mathbb{N}}$, identificamos a f con la tupla infinita $(f(0), f(1), f(2), \ldots)$.

Ahora vamos a definir una función

$$\varphi : 2^{\mathbb{N}} \to \mathcal{P}(\mathbb{N}).$$

[4] No confundir con el Teorema de Cantor-Schröder-Bernstein (TCSB), estudiado en la § 5.2, arriba.

Esto es, φ *transforma funciones en conjuntos*. Dada $f \in 2^{\mathbb{N}}$, la definición de $\varphi(f)$ es la siguiente:

$$\varphi(f) = f^{-1}[\{1\}] = \{n \in \mathbb{N} : f(n) = 1\}.$$

Sea ahora $\psi : \mathcal{P}(\mathbb{N}) \to 2^{\mathbb{N}}$, la función definida así: $\psi(S) = f_S$, en donde:

$$f_S(n) = \begin{cases} 1 & \text{si } n \in S; \\ 0 & \text{si } x \notin S. \end{cases}$$

Dejamos al lector la tarea de verificar que $\varphi \circ \psi = \mathrm{ID}_{\mathcal{P}(\mathbb{N})}$ y $\psi \circ \varphi = \mathrm{ID}_{2^{\mathbb{N}}}$. Por el Teorema 4.56, concluimos que $|2^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$. ∎

Teorema 5.31. $\mathbb{R}$ no es enumerable. En otras palabras, $|\mathbb{N}| < |\mathbb{R}|$.

Prueba. Sea $2^{\mathbb{N}}$ el conjunto considerado en el Lema 5.30; asimismo, sea $\tau : 2^{\mathbb{N}} \to [0,1)$ la función definida así:

$$\tau(f) = 0, f(0)f(1)f(2)\cdots \in [0,1).$$

Por ejemplo, si $f = (0,1,0,1,0,0,0,0,\dots)$, entonces $\tau(f)$ es el siguiente número real:

$$0,0101000\dots$$

Veamos que τ es inyectiva: sean $f, f' \in 2^{\mathbb{N}}$, con $f \neq f'$. Sea n el mínimo número natural tal que $f(n) \neq f'(n)$. Hay dos casos:

(i) $f(n) = 0$ y $f'(n) = 1$: si definimos ahora

$$r := 0, f(0)f(1)\dots f(n-1)f(n)5111\dots,$$

entonces claramente $\tau(f) < r < \tau(f')$, luego $\tau(f) \neq \tau(f')$.

(ii) $f(n) = 1$ y $f'(n) = 0$: si razonamos análogamente a como se hizo en el caso (i), concluimos que $\tau(f) \neq \tau(f')$.

Así, en cualquier caso tenemos que $\tau(f) \neq \tau(f')$. Concluimos que $|2^{\mathbb{N}}| \leq |[0,1)|$. Además, $[0,1) \subseteq \mathbb{R}$. Luego

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}| \leq |[0,1)| \leq |\mathbb{R}|$$

y, de este modo, $|\mathbb{N}| < |\mathbb{R}|$. ∎

El lector se preguntará si el cardinal de $\mathbb{R}$ es exactamente el cardinal de $\mathcal{P}(\mathbb{N})$. La respuesta es afirmativa y en el ejercicio 10 sugerimos una manera de demostrarlo. Este es un hecho interesante: el cardinal de $\mathbb{R}$ es igual al cardinal del conjunto $\mathcal{P}(\mathbb{N})$. Para resumir y complementar el panorama, en el siguiente teorema listamos varios conjuntos cuyo cardinal es igual al cardinal del conjunto de los numeros reales:

Teorema 5.32. Sean a y b números reales cualesquiera, con $a < b$, y sea A un conjunto a lo sumo enumerable. Los siguientes conjuntos tienen todos el mismo cardinal, es decir, son equipotentes:

(a) $\mathbb{R}$,	(e) $[0,1)$,	(i) $(a,b]$,	(m) $[a,\infty)$,
(b) $\mathcal{P}(\mathbb{N})$,	(f) $(0,1)$,	(j) $[a,b]$,	(n) $(-\infty,b]$,
(c) $2^{\mathbb{N}}$	(g) (a,b),	(k) (a,∞),	(ñ) $\mathbb{R}^+$,
(d) $(0,1]$,	(h) $[a,b)$,	(l) $(-\infty,b)$,	(o) $\mathbb{R} \setminus A$.

Prueba. En el ejercicio 10, el lector demostrará que $|\mathbb{R}| = |[0,1)| = |\mathcal{P}(\mathbb{N})|$ y en el ejercicio 8, el lector demostrará que $|\mathbb{R}| = |\mathbb{R} \setminus A|$. Demostremos otras igualdades de cardinales:

- $|(0,1]| = |[0,1)|$: basta considerar la función $f : (0,1] \to [0,1)$ que fija todo punto, salvo el 1, que lo envía al 0. Conjuntistamente, $f = \text{ID}_{(0,1)} \cup \{(1,0)\}$. Dejamos al lector la tarea de comprobar que f es una biyección.
- $|[0,1)| = |(0,1)|$: sea $f : [0,1) \to (0,1)$ la función que envía 0 a $\frac{1}{2}$, $\frac{1}{2}$ a $\frac{1}{3}$, $\frac{1}{3}$ a $\frac{1}{4}$, etc., y se comporta como la identidad en el resto de los puntos. Dejamos al lector el trabajo de definir más precisamente a f y comprobar que es una biyección.
- $|(0,1)| = |(a,b)|$: sea $f : (0,1) \to (a,b)$ la función definida como $f(x) = (b-a)x + a$. El lector debe verificar que f es una biyección.

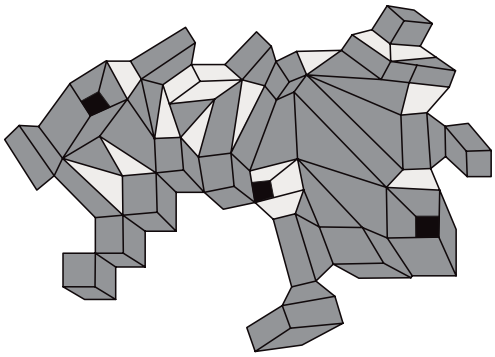
Con métodos análogos a los que acabamos de utilizar podemos ver fácilmente que cada uno de los demás conjuntos tiene el mismo cardinal que alguno que ya hemos considerado (véase el ejercicio 4). Gracias a la simetría y transitividad de la relación de equipotencia, concluimos, por lo tanto, que *todos* los conjuntos listados anteriormente son equipotentes entre sí. ∎

Corolario 5.33. Sea $S \subseteq \mathbb{R}$. Si S contiene un intervalo abierto, entonces $|S| = |\mathbb{R}|$.

Prueba. Sean $a, b \in \mathbb{R}$, con $a < b$, tales que $(a,b) \subseteq S$. Si utilizamos el Teorema 5.32 concluimos que $|\mathbb{R}| = |(a,b)| \leq |S| \leq |\mathbb{R}|$, y, por el TCSB, tenemos en consecuencia que $|S| = |\mathbb{R}|$. ∎

Un interesante asunto consiste en preguntarse si vale el recíproco del corolario anterior: ¿si $S \subseteq \mathbb{R}$ y $|S| = |\mathbb{R}|$, entonces S contiene un intervalo abierto? El lector podrá indagar esta cuestión por sí mismo.

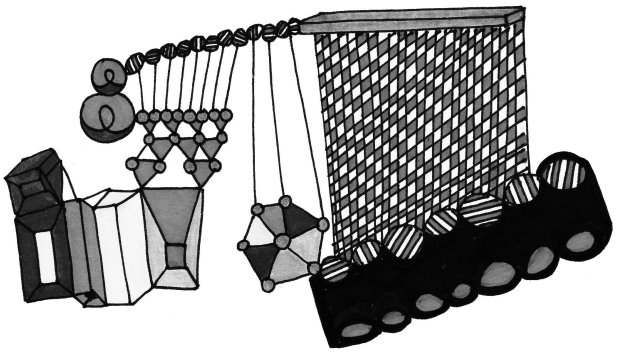
Ejercicios



1. Demuestre que si A es un conjunto infinito no enumerable y $A \subseteq B$, entonces B es infinito no enumerable.
2. Sean X un conjunto infinito no enumerable y $S \subseteq X$. Demuestre que S es infinito no enumerable o S^c es infinito no enumerable.
3. Utilice el ejercicio anterior para demostrar que el conjunto de los *números irracionales* $I := \mathbb{R} \setminus \mathbb{Q}$ es infinito no enumerable.
4. Sean $a, b \in \mathbb{R}$ con $a < b$. Construya biyecciones explícitas entre los siguientes conjuntos, y demuestre que en realidad son biyecciones:
   (a) $[0,1)$ y $(0,1)$;
   (b) $[0,1]$ y $(0,1)$;
   (c) $(0,1)$ y (a,b);
   (d) $(0,1)$ y $(0,\infty)$;
   (e) $(0,\infty)$ y (a,∞);
   (f) $(0,\infty)$ y $(-\infty,0)$.
5. Construya una biyección explícita entre $\mathbb{R}$ e $I = \mathbb{R} \setminus \mathbb{Q}$. (*Ayuda*: sea la función $f : \mathbb{Q} \to \mathbb{N}$ una biyección. Defina $g : \mathbb{R} \to I$ de modo que $g(x) = 2f(x)\pi$ para $x \in \mathbb{Q}$, $g(x) = (2k+1)\pi$ si $x = k\pi$ (con $k \in \mathbb{N}^*$), y $g(x) = x$ para otros valores de x. Demuestre que g es una biyección.)
6. Sea $\mathbb{N}^{\mathbb{N}}$ el conjunto de sucesiones de números naturales:
   $$\mathbb{N}^{\mathbb{N}} = \{ (a_n)_{n\in\mathbb{N}} : \forall n \in \mathbb{N}, a_n \in \mathbb{N} \}.$$
   Demuestre que $\mathbb{N}^{\mathbb{N}}$ es un conjunto infinito no enumerable. (*Ayuda*: encuentre una función inyectiva $\mathcal{P}(\mathbb{N}) \to \mathbb{N}^{\mathbb{N}}$.)
7. Sea $\mathcal{F}$ el conjunto de las sucesiones finalmente nulas de números naturales, es decir, el conjunto de todas las sucesiones $(a_n)_{n\in\mathbb{N}}$ que cumplen con la siguiente propiedad:
   $$\begin{array}{c}\text{para todo } n \in \mathbb{N},\ a_n \in \mathbb{N} \text{ y existe } m \in \mathbb{N} \text{ tal que}\\ \text{para todo } n \in \mathbb{N} \text{ si } n \geq m, \text{ entonces } a_n = 0.\end{array}$$
   Note que $\mathcal{F} \subseteq \mathbb{N}^{\mathbb{N}}$. Demuestre que $\mathcal{F}$ es un conjunto enumerable.

8. Sea A un subconjunto a lo sumo enumerable de $\mathbb{R}$. Demuestre que $|\mathbb{R}| = |\mathbb{R} \setminus A|$.
9. Demuestre que existen conjuntos X_n (para $n \in \mathbb{N}$), tales que cada X_n es infinito, $X_n \subseteq X_{n+1}$ y $|X_n| < |X_{n+1}|$.
10. El objetivo de este ejercicio es demostrar que $\mathbb{R}$ y $\mathcal{P}(\mathbb{N})$ son equipotentes. Para ello, y en virtud del TCSB, es suficiente demostrar que $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$ y $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$. Si revisamos en detalle el Teorema 5.31, obtenemos una desigualdad. Para la otra desigualdad, ofrecemos una serie de pasos:
    (a) Demuestre que $|[0,1)| \leq |\mathcal{P}(\mathbb{N})|$.
    (b) Demuestre que $|\mathbb{R}^+| \leq |\mathcal{P}(\mathbb{N})|$. (*Ayuda*: sea $\varphi : [0,1) \to \mathcal{P}(\mathbb{N})$ una función inyectiva, que existe por el sub-ejercicio anterior. Considere la función $\psi : \mathbb{R}^+ \to \mathcal{P}(\mathbb{N})$ dada por
    $$\psi(n+r) = \{2n+1\} \cup \{2k : k \in \varphi(r)\},$$
    donde $n \in \mathbb{N}$, $r \in [0,1)$. Demuestre que ψ es inyectiva.)
    (c) Demuestre que $|\mathbb{R}| \leq |\mathbb{R}^+|$. (*Ayuda*: utilice una idea similar a la utilizada en la parte (b).)
    (d) Concluya el resultado.
11. Sea $C = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ el círculo unitario del plano. Demuestre que $|C| = |\mathbb{R}|$.
12. Demuestre que $|\mathbb{R}^2| = |\mathbb{R}|$. (*Ayuda*: demuestre que $|2^{\mathbb{N}} \times 2^{\mathbb{N}}| = |2^{\mathbb{N}}|$.)
13. Demuestre que para todo $n \in \mathbb{N}^*$, $|\mathbb{R}^n| = |\mathbb{R}|$. (*Ayuda*: utilice el ejercicio 12 y el Teorema 5.6.)
14. Demuestre que $|\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|$.
15. ¿Verdadero o falso? Si $S \subseteq \mathbb{R}$ y $|S| = |\mathbb{R}|$, entonces S contiene un intervalo abierto, esto es, existen $a, b \in \mathbb{R}$ tales que $a < b$ y $(a,b) \subseteq S$.
16. Sea $f : \mathbb{R} \to \mathbb{R}$ una función continua y estrictamente creciente. Además, suponga que
    $$\lim_{x \to \infty} f(x) = \infty, \text{ y}$$
    $$\lim_{x \to -\infty} f(x) = -\infty.$$
    Demuestre que f es una biyección. (Consulte en [10] las definiciones utilizadas en este ejercicio.)

Proyecto: Monotonía de la relación de equipotencia



En este proyecto demostraremos que ciertas operaciones básicas conjuntistas, como son el producto cartesiano, la unión disjunta, el producto generalizado, la exponenciación y la operación "partes de", son monótonas con respecto a la equipotencia. Por ejemplo, si $|A| = |A'|$ y $|B| = |B'|$, entonces $|A \times B| = |A' \times B'|$ (Teorema 5.6). Ejemplos de operaciones que *no* son monótonas con respecto de la equipotencia son la unión, la intersección y el complemento.

Problemas

1. Dé un ejemplo de conjuntos A, B, C y D tales que se cumpla que $|A| = |B|$ y $|C| = |D|$, pero $|A \cup C| \neq |B \cup D|$.
2. Dé un ejemplo de conjuntos A, B, C y D tales que se cumpla que $|A| = |B|$ y $|C| = |D|$ pero $|A \cap C| \neq |B \cap D|$.
3. Dé un ejemplo de conjuntos A, $B \subseteq \mathcal{U}$ tales que se cumpla que $|A| = |B|$ pero $|A^c| \neq |B^c|$.
4. Dados dos conjuntos A y B, definimos su *unión disjunta* como

$$A \sqcup B := (A \times \{0\}) \cup (B \times \{1\}).$$

   Un elemento $y \in A \sqcup B$ será de la forma $y = (x, i)$, en donde $i = 0, 1$. Coloquialmente hablando, si $i = 0$, entonces y fue construido a partir de un elemento en A; y si $i = 1$, entonces y fue construido a partir de un elemento en B.

   (a) Sea $A = \{3, 4, 5, 6\}$, $B = \{5, 6, 7\}$. Calcule $A \sqcup B$ y determine el número de elementos de este conjunto.

   (b) Demuestre que en general $|A \cup B| \leq |A \sqcup B|$.

(c) Demuestre el Teorema de Monotonía de Equipotencias para uniones disjuntas: si $|A| = |B|$ y $|C| = |D|$ entonces se tiene que $|A \sqcup C| = |B \sqcup D|$.

5. Para este ejercicio considere la siguiente definición:

   Definición. Sea $\{A_i : i \in I\}$ un conjunto de conjuntos. Definimos la *unión disjunta de los* A_i, y la simbolizamos $\bigsqcup_{i\in I} A_i$, así:

   $$\bigsqcup_{i\in I} A_i := \bigcup_{i\in I} A_i \times \{i\}.$$

   (Note que los elementos de este conjunto son pares de la forma (a, i), donde $a \in A_i$.)

   Demuestre el Teorema de Monotonía de Equipotencias para unión disjunta generalizada: a saber, si $|A_i| = |B_i|$ para todo $i \in I$, entonces $|\bigsqcup_{i\in I} A_i| = |\bigsqcup_{i\in I} B_i|$.

6. Recordemos que, dados los conjuntos X y Y, definimos X^Y como

   $$X^Y := \{f : (f : Y \to X)\},$$

   es decir, el conjunto de todas las funciones $f : X \to Y$. Sean A_0, A_1, B_0, y B_1 conjuntos tales que $|A_0| = |A_1|$ y $|B_0| = |B_1|$. Demuestre que $|B_0^{A_0}| = |B_1^{A_1}|$.

7. Demuestre que si $|A| = |B|$, entonces $|\mathcal{P}(A)| = |\mathcal{P}(B)|$.

8. Sea $\{A_i : i \in I\}$ un conjunto de conjuntos. Definimos el *producto de los* A_i, y lo simbolizamos $\prod_{i\in I} A_i$, como el conjunto de todas las funciones f tales que $\text{DOM}(f) = I$ y para todo $i \in I$, $f(i) \in A_i$.

   (a) Sean $I = \{0, 1, 2\}$, $A_0 = \{3\}$, $A_1 = \{3, 4\}$, $A_3 = \{5, 6, 7\}$. Calcule el conjunto $\prod_{i\in I} A_i$.

   (b) Demuestre el Teorema de monotonía de equipotencias para el producto: si para todo $i \in I$, $|A_i| = |B_i|$ entonces

   $$\left|\prod_{i\in I} A_i\right| = \left|\prod_{i\in I} B_i\right|.$$

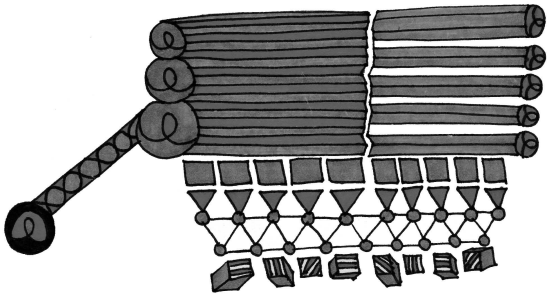
9. Sean A y B conjuntos. Demuestre que $|\mathcal{P}(A \times B)| = |\mathcal{P}(B)^A|$.

10. Sean A, B y C conjuntos. Demuestre las siguientes propiedades de los exponentes:

    (a) $|(A^B)^C| = |A^{B\times C}|$.

    (b) $|A^B \times A^C| = |A^{B\sqcup C}|$.

Lecturas adicionales

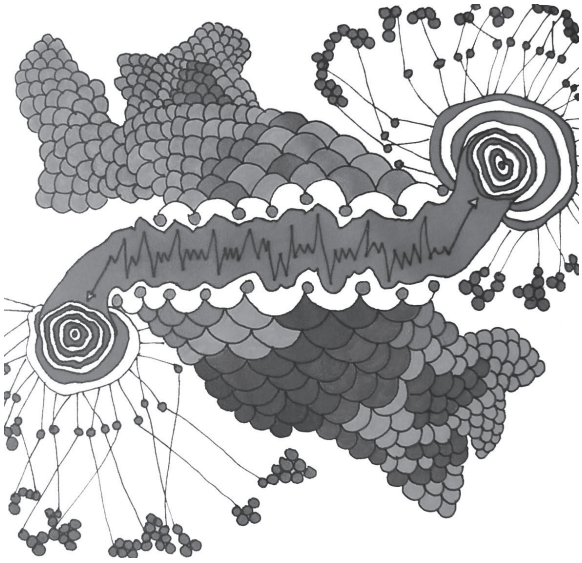


Se recomienda consultar las siguientes lecturas, con miras a profundizar en algunos de los temas tratados en este capítulo:

- Para más información sobre biyecciones y cardinales, consulte [2], § 1.5; [4], § 4.1.
- Para más información sobre conjuntos finitos y enumerables, consulte [2], § 1.6; [4], §§ 4.2–3.
- Para más información sobre conjuntos no enumerables, consulte [4], § 4.6.

CAPÍTULO 6

ESTRUCTURAS MATEMÁTICAS



Estructura es aquello que es preservado por isomorfismos...

A grandes rasgos, una estructura matemática consiste en un conjunto A, llamado *conjunto base*, junto con una o varias construcciones matemáticas que involucran a A y ciertas propiedades que verifican estas construcciones. Estas propiedades se formulan mediante axiomas. Las construcciones a las que nos referimos abarcan relaciones n-arias sobre A, esto es, subconjuntos de A^n, funciones $f : A^n \to A$ llamadas *operaciones n-arias*, funciones $f : A^n \to \mathbb{R}$, subconjuntos de $\mathcal{P}(A)$, etc.

En este capítulo daremos ejemplos de varias estructuras matemáticas: órdenes, grupos (que estudiaremos con cierto detalle), álgebras de Boole, espacios métricos y espacios topológicos. Además estudiaremos isomorfismos entre algunas de estas estructuras, lo cual formaliza la noción intuitiva de que dos construcciones matemáticas sean estructuralmente equivalentes o tengan la misma estructura.

§ 6.1 Conceptos fundamentales

Conjuntos parcialmente ordenados

Como hemos visto en los anteriores capítulos de este libro, un conjunto parcialmente ordenado (A, R) consiste en un conjunto A junto con una relación R sobre A que cumple con los siguientes tres axiomas: reflexividad, antisimetría y transitividad.

Por ejemplo, la estructura $(\mathbb{Z}^*, |_{\mathbb{Z}})$ es un orden parcial. Aquí,

$$|_{\mathbb{Z}} = \{(n, m) \in \mathbb{Z}^2 : n \mid m\}.$$

Una estructura parcialmente ordenada distinta de $(\mathbb{Z}, |_{\mathbb{Z}})$ es $(\mathbb{N}^*, |_{\mathbb{N}^*})$, en donde $|_{\mathbb{N}^*}$ denota la relación *divide a*, restringida al conjunto $\mathbb{N}^*$:

$$|_{\mathbb{N}^*} = \{(n, m) \in (\mathbb{N}^*)^2 : n \mid m\}.$$

Las anteriores estructuras son distintas. Sin embargo, en algún sentido una de ellas "vive dentro de la otra", ya que no sólo $\mathbb{N}^* \subseteq \mathbb{Z}$, sino además la relación $|_{\mathbb{Z}}$ *coincide* con la relación $|_{\mathbb{N}^*}$ en los elementos de $\mathbb{N}^*$. Esto lo expresaremos diciendo que $(\mathbb{N}^*, |_{\mathbb{N}^*})$ es una *subestructura* de $(\mathbb{Z}, |_{\mathbb{Z}})$. En este caso, un *suborden*.

Subestructura

Definición 6.1 (Subestructura). Sean (A_1, R_1) y (A_2, R_2) dos estructuras relacionales donde $R_1 \subseteq A_1^2$ y $R_2 \subseteq A_2^2$. Diremos que (A_1, R_1) es una *subestructura* de (A_2, R_2), si $A_1 \subseteq A_2$ y, además, R_1 y R_2 coinciden sobre A_1, es decir, si para todo $a, b \in A_1$, aR_1b si y sólo si aR_2b. Conjuntistamente, si $R_1 = A_1^2 \cap R_2$.

Ejemplo 6.2. Consideremos la estructura (A, R), la cual se define como $A = \{2, 5, 7\}$ y $R = \{(2, 5), (2, 7), (5, 7)\}$. Entonces (A, R) es una subestructura de $(\mathbb{N}, <)$, pero no es una subestructura de $(\mathbb{N}, \leq)$, porque —por ejemplo— $(2, 2) \in \leq \setminus R$.

Ejemplo 6.3. Consideremos la estructura $(\mathbb{N}, |_{\mathbb{N}})$. Aunque $\mathbb{N} \subseteq \mathbb{Z}$ y $|_{\mathbb{N}} \subseteq \leq$ —o, lo que es equivalente, si $n \mid m$, entonces $n \leq m$—, la estructura $(\mathbb{N}, |_{\mathbb{N}})$ no es una subestructura de $(\mathbb{Z}, \leq)$, ya que en el conjunto $\mathbb{N}$ las relaciones $|_{\mathbb{N}}$ y $\leq$ son distintas; por ejemplo, se tiene que $4 \leq 5$ pero $4 \nmid 5$.

Álgebras de Boole

Una clase particularmente interesante de estructuras es la clase formada por las álgebras de Boole. Antes de definir este concepto, veamos un ejemplo representativo del mismo:

Ejemplo 6.4. Sea $\mathcal{U}$ un conjunto. A partir de $\mathcal{U}$ formamos la estructura dada por

$$\mathbb{B} = (B, 1_{\mathbb{B}}, 0_{\mathbb{B}}, +, \cdot, \neg)$$

de la siguiente manera:

(a) $B := \mathcal{P}(\mathcal{U})$, el conjunto base de la estructura;

(b) $1_{\mathbb{B}} = \mathcal{U} \in B$ y $0_{\mathbb{B}} = \varnothing \in B$;

(c) dados $E, F \in B$, $E + F := E \cup F \in B$;

(d) dados $E, F \in B$, $E \cdot F := E \cap F \in B$; y

(e) dado $E \in B$, $\neg E := \mathcal{U} \setminus E = E^c \in B$.

En otras palabras, $\mathbb{B}$ es la estructura

$$\mathbb{B} = (\mathcal{P}(\mathcal{U}), \mathcal{U}, \varnothing, \cup, \cap, {}^c).$$

En el capítulo 1 demostramos que para $a, b, c \in B$ se cumplen las siguientes propiedades:

(A1) *conmutatividad*: $a \cup b = b \cup a$; $a \cap b = b \cap a$;

(A2) *asociatividad*: $a \cup (b \cup c) = (a \cup b) \cup c$; $a \cap (b \cap c) = (a \cap b) \cap c$;

(A3) *absorción*: $a \cap (a \cup b) = a$; $a \cup (a \cap b) = a$;

(A4) *distribución*: $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$; $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$;

(A5) *todo o nada*: $a \cap a^c = \varnothing$; $a \cup a^c = \mathcal{U}$.

Definición 6.5 (Algebra de Boole). Un *álgebra de Boole*,

Álgebra de Boole

$$\mathbb{B} = (B, 0_{\mathbb{B}}, 1_{\mathbb{B}}, +, \cdot, \neg),$$

está compuesta por un conjunto B, los elementos $0_{\mathbb{B}}, 1_{\mathbb{B}} \in B$, y las funciones $+ : B^2 \to B$, $\cdot : B^2 \to B$, $\neg : B \to B$, sujetas a los siguientes axiomas (donde $a, b, c \in B$):

(A1) *conmutatividad*: $a + b = b + a$; $a \cdot b = b \cdot a$;

(A2) *asociatividad*: $a + (b + c) = (a + b) + c$; $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(A3) *absorción*: $a \cdot (a + b) = a$; $a + (a \cdot b) = a$;

(A4) *distribución*: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$; $a + (b \cdot c) = (a + b) \cdot (a + c)$;

(A5) *todo o nada*: $a \cdot \neg a = 0_{\mathbb{B}}$; $a + \neg a = 1_{\mathbb{B}}$.

Como hemos visto, para todo conjunto $\mathcal{U}$ tenemos que la estructura

$$\mathbb{B} = (\mathcal{P}(\mathcal{U}), \mathcal{U}, \varnothing, \cup, \cap, {}^c)$$

Álgebra de subconjuntos

es un álgebra de Boole, llamada el *álgebra de subconjuntos de* $\mathcal{U}$.

Ejemplo 6.6. Sea $\mathbb{B} = (\{0,1\}, 1, 0, \text{MÁX}, \text{MÍN}, \neg(x) = 1 - x)$. Entonces $\mathbb{B}$ es un álgebra de Boole.

Espacios métricos

En matemáticas, el conjunto de los números reales permite medir la distancia entre dos elementos de diversos conjuntos ($\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^3$). Por ejemplo, en $\mathbb{R}^2$ la distancia euclídea entre los puntos $(1,3)$ y $(2,5)$ está dada por

$$d((1,3),(2,5)) = \sqrt{(1-2)^2 + (3-5)^2} = \sqrt{5}.$$

Esta idea conduce al concepto más general de *espacio métrico*.

Espacio métrico

Definición 6.7 (Espacio métrico). Un *espacio métrico* (A, d) consiste en un conjunto A y una función llamada *distancia* $d : A^2 \to \mathbb{R}$, sujeta a los siguientes axiomas:

(A1) Dados $a, b \in A$, $d(a,b) \geq 0$.

(A2) Dados $a, b \in A$, $d(a,b) = 0$ si y sólo si $a = b$.

Simetría

(A3) *Simetría*: dados $a, b \in A$, se tiene que $d(a,b) = d(b,a)$.

Desigualdad triangular

(A4) *Desigualdad triangular*: dados $a, b, c \in A$, se tiene que

$$d(a,c) \leq d(a,b) + d(b,c).$$

La expresión $d(a,b)$ se lee: "la distancia entre a y b".

Muchas veces la definición de una estructura trae consigo nociones de conjuntos especiales. En el caso de los espacios métricos, es natural definir la *vecindad* de un punto:

$N_\varepsilon(a)$: Vecindad

Definición 6.8. Sea (A, d) un espacio métrico. Dado $a \in A$ y $\varepsilon \in \mathbb{R}^+$ definimos la *vecindad de radio* ε *centrada en* a, y la notamos $N_\varepsilon(a)$, así:

$$N_\varepsilon(a) = \{x \in A : d(a,x) < \varepsilon\} \subseteq A.$$

Ejemplo 6.9. Sea $A = \mathbb{R}$ y sea $d : A^2 \to \mathbb{R}$ la función definida como $d(a,b) = |b-a|$. Puede verse que (A,d) es un espacio métrico. Por ejemplo, $d(2,7) = d(7,2) = 5$ y para todo $a \in A$, $d(a,-a) = 2|a|$. Además, la vecindad de radio 2 centrada en 7 es

$$N_2(7) = \{x \in \mathbb{R} : |x-7| < 2\} = (5,9).$$

☞ **Antes de seguir leyendo**

Sea (A,d) un espacio métrico y sea $a \in A$. Demuestre que:

1. Si $\varepsilon_1 \leq \varepsilon_2$, entonces $N_{\varepsilon_1}(a) \subseteq N_{\varepsilon_2}(a)$.
2. $\bigcup_{\varepsilon>0} N_\varepsilon(a) = A$.
3. $\bigcap_{\varepsilon>0} N_\varepsilon(a) = \{a\}$.

Espacios topológicos

Definición 6.10 (Espacio topológico). Un espacio topológico (X,τ) consiste en un conjunto X y un conjunto $\tau \subseteq \mathcal{P}(X)$ que cumple con los siguientes axiomas: *Espacio topológico*

(A1) $X \in \tau$ y $\varnothing \in \tau$;

(A2) si $\{A_i : i \in I\} \subseteq \tau$, entonces $\bigcup_{i\in I} A_i \in \tau$;

(A3) si $A_1, A_2 \in \tau$, entonces $A_1 \cap A_2 \in \tau$.

El conjunto τ es llamado una *topología* sobre X. A los elementos $A \in \tau$ los llamaremos *abiertos* de τ. *Topología* *Abiertos*

Construir un espacio topológico consiste esencialmente en selecionar un conjunto base X y ciertos subconjuntos suyos, incluyendo siempre a X y a $\varnothing$, de modo que cumplan con ciertas propiedades de *clausura* (las propiedades A2 y A3 en la definición anterior).

Ejemplo 6.11. Sea $X = \{0,1\}$ y sea $\tau \subseteq \mathcal{P}(X)$ el siguiente conjunto:

$$\tau = \{\varnothing, \{1\}, \{0,1\}\}.$$

Es fácil verificar que τ cumple con los tres axiomas de un espacio topológico. Luego (X,τ) es un espacio topológico, llamado el *Espacio de Sierpiński*.

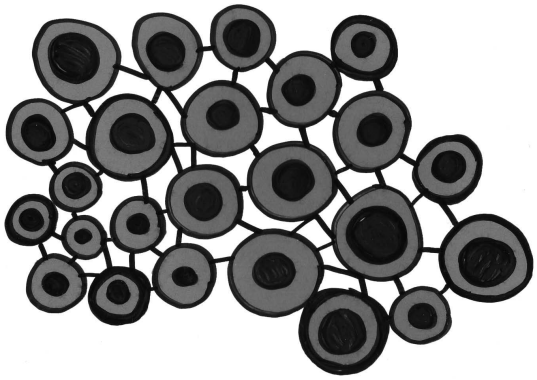
Ejemplo 6.12. Sea $X = \mathbb{R}^2$, con la distancia euclídea. Dado un conjunto $A \subseteq X$, diremos que A es abierto, si para todo $a_0 \in A$ existe un número real $\varepsilon > 0$ tal que $N_\varepsilon(a) \subseteq A$ (véase la Definición 6.8). Dicho de otro modo, "todos los puntos ε-cercanos a a pertenecen a A". Sea τ el conjunto de todos los conjuntos abiertos $A \subseteq X$. Puede demostrarse que (X, τ) es un espacio topológico.

☞ **Antes de seguir leyendo**

(a) Sea $X = \{1, 2, 3\}$. Defina una topología τ sobre X, tal que τ tenga exactamente cinco abiertos.

(b) Sea $\tau = \{S \in \mathcal{P}(\mathbb{N}) : S = \varnothing \vee \mathbb{N} \setminus S \text{ es finito}\}$. Demuestre que $(\mathbb{N}, \tau)$ es un espacio topológico.

Otras estructuras matemáticas

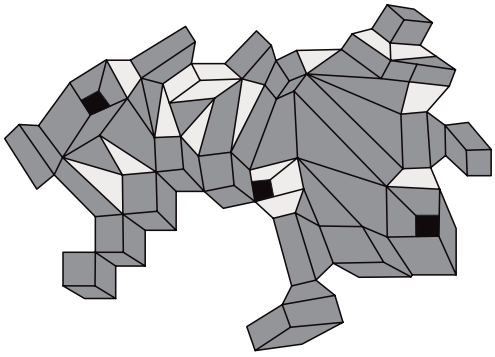


Listamos a modo de referencia algunas de las estructuras matemáticas fundamentales, junto con algunas de las ramas que las estudian o utilizan como instrumento. Cabe mencionar que todas ellas pueden definirse en términos conjuntistas.

Estructuras	Ramas asociadas
Órdenes parciales y lineales	Teoría de conjuntos
Grafos	Teoría de grafos, Combinatoria
Grupos, anillos, campos	Álgebra

Álgebras de Heyting	Álgebra, Lógica
Álgebras de Boole	Álgebra, Lógica
Geometrías axiomáticas	Geometría
Módulos, espacios vectoriales	Álgebra lineal
Espacios métricos	Análisis real
Espacios topológicos	Topología, Análisis, Lógica
Sigma-álgebras, espacios de medida	Teoría de la medida, Probabilidad
Espacios normados	Análisis funcional
Variedades topológicas y diferenciales	Topología, Análisis, Geometría diferencial
Categorías	Álgebra, Geometría, Lógica
Matroides	Combinatoria

Ejercicios

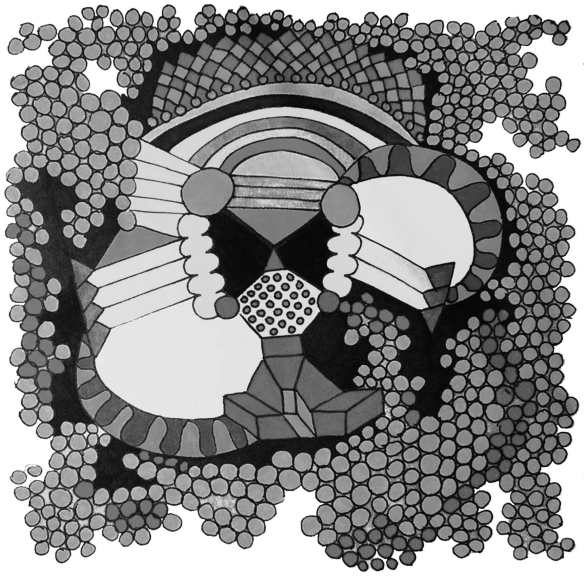


1. Sea A un conjunto con tres elementos. Determine el número de formas de ordenar parcialmente a A.
2. Sea A un conjunto con cuatro elementos. Determine el número de formas esencialmente distintas (esto es, no isomorfas) de ordenar parcialmente a A.
3. Considere la siguiente función $d : \mathbb{N}^2 \to \mathbb{R}$:

$$d(a,b) = \begin{cases} 0 & \text{si } a = b; \\ 1 & \text{si } a \neq b. \end{cases}$$

   Demuestre que la estructura $(\mathbb{N}, d)$ es un espacio métrico.

4. Demuestre que para todo conjunto A, $(A, \{\varnothing, A\})$ es un espacio topológico.
5. Sea $\mathcal{U}$ un conjunto finito y sea $d : \mathcal{P}(\mathcal{U})^2 \to \mathbb{R}$ la función definida de esta manera:
$$d(E,F) = |E \setminus F| + |F \setminus E| \qquad (E,F \subseteq \mathcal{U}).$$
Demuestre que la estructura $(\mathcal{P}(\mathcal{U}), d)$ es un espacio métrico.
6. Sea (A,d) un espacio métrico. Diremos que (A,d) es *pleno* si cumple con el siguiente axioma:
(A5) Para todo $a \in A$ y $\varepsilon \in \mathbb{R}$, con $\varepsilon > 0$, existe $b \in A$, tal que $a \neq b$ y $d(a,b) < \varepsilon$.
Demuestre que a partir de los axiomas de espacios métricos no puede deducirse el axioma A5 ni su negación. Esto demuestra que el axioma A5 es *independiente* de los axiomas de espacios métricos. (*Ayuda*: demuestre que existen espacios métricos plenos y que existen espacios métricos que no son plenos.)
7. Sea $(A, \leq)$ una estructura parcialmente ordenada. Dado $E \subseteq A$, diremos que E es *hereditario* si dados $a, b \in A$, si $a \leq b$ y $a \in E$, entonces $b \in E$. Sea
$$\tau = \{E \in \mathcal{P}(A) : E \text{ es hereditario}\}.$$
Demuestre que (A, τ) es un espacio topológico.
8. Sea (X, τ) un espacio topológico. Dado $C \subseteq X$, diremos que C es *cerrado* si $C^c \in \tau$. Demuestre:
   (a) X y $\varnothing$ son cerrados.
   (b) Si $\{A_i : i \in I\}$ es una colección de conjuntos cerrados, entonces $\bigcap_{i \in I} A_i$ es un conjunto cerrado.
   (c) Si A_1 y A_2 son cerrados, entonces $A_1 \cup A_2$ es cerrado.
9. Sea (X, τ) un espacio topológico. Demuestre que para todo $n \in \mathbb{N}^*$ se tiene que si $A_1, \ldots, A_n \in \tau$, entonces $A_1 \cap \ldots \cap A_n \in \tau$.
10. Sea (A,d) un espacio métrico. Dado $S \subseteq A$, diremos que S es *agradable* si y sólo si para todo $x \in S$ existe $\varepsilon > 0$, tal que $N_\varepsilon(x) \subseteq S$. Sea τ la colección de todos los subconjuntos agradables de A. Demuestre que (A, τ) es un espacio topológico. Demuestre también que para todo S, $S \in \tau$ si y sólo si S es de la forma $\bigcup_{i \in I} N_{\varepsilon_i}(x_i)$, en donde para todo $i \in I$ se tiene que $\varepsilon_i \in \mathbb{R}^+$ y $x_i \in A$.



§ 6.2 Grupos

En el conjunto de los números enteros, la suma + es una función que transforma un par ordenado de números enteros (a, b) en un número entero $c = a + b$. Esto es,

$$+ : \mathbb{Z}^2 \to \mathbb{Z}.$$

Por ejemplo, $+(2,6) = 8$, $+(5,-6) = -1$ y $+(4,0) = 4$. En vez de escribir la suma en la notación funcional *prefija* $+(a,b)$, esto es, escribiendo el símbolo de suma antes de los elementos que se operan, por costumbre escribimos la suma en la notación *infija*: $a + b$, es decir, en donde utilizamos el símbolo de la función en el medio de los elementos que se operan. Así, los ejemplos anteriores se transforman en $2 + 6 = 8$, $5 + -6 = -1$ y $4 + 0 = 4$. En esta sección utilizaremos la notación infija.

Notación prefija

Notación infija

Definición 6.13 (Operación binaria). Sea A un conjunto. Diremos que $\odot$ es una *operación binaria* sobre A, si $\odot$ es una función que cumple que $\text{DOM}(\odot) = A^2$ e $\text{IMG}(\odot) \subseteq A$.

Operación binaria

En otras palabras, una operación binaria sobre A es una función $\odot : A^2 \to A$. Dicho informalmente, "al operar con elementos de A obtenemos un elemento de A".

Ejemplo 6.14. Sean $A = \{n \in \mathbb{N} : n \leq 10\}$, y $\odot$ la función *máximo*, dada por $a \odot b = \text{MÁX}(a, b)$ (para $a, b \in A$). Tenemos que $\odot$ es una operación binaria sobre A, pues si $a, b \in A$, entonces $a \odot b = \text{MÁX}(a, b) \in \{a, b\} \subseteq A$. Por lo tanto, $a \odot b \in A$.

Identidad

Definición 6.15 (Identidad). Sea A un conjunto y sea $\odot$ una operación binaria sobre A. Dado $e \in A$, diremos que e es una *identidad* con respecto a $\odot$ si para todo $x \in A$ se tiene que $x \odot e = e \odot x = x$. En otras palabras, cuando e se opera con cualquier elemento x y en cualquier orden, deja *idéntico* el valor original de x.

Por ejemplo, en el conjunto $\mathbb{R}$ el elemento 0 es una identidad con respecto a la operación suma, debido a que para todo $x \in \mathbb{R}$ tenemos que $x + 0 = 0 + x = x$. Asimismo, en $\mathbb{R}$ el elemento 1 es una identidad con respecto a la operación multiplicación, ya que para todo $x \in \mathbb{R}$ tenemos que $(x)(1) = (1)(x) = x$.

☞ **Antes de seguir leyendo**

1. Sea $\odot$ la operación binaria sobre $\mathbb{N}$ definida por $a \odot b := \text{MÁX}(a, b)$. ¿Existen identidades para esta operación?
2. Sea $\odot$ la operación binaria sobre $\mathbb{N}$ definida por $a \odot b = \text{MÍN}(a, b)$. ¿Existen identidades para esta operación?

Vamos ahora a definir el concepto de *grupo*, un importante ejemplo de estructura matemática:

Grupo

Definición 6.16 (Grupo). Sea G un conjunto y sea $\odot : G \times G \to G$ una operación binaria sobre G. Diremos que la estructura $(G, \odot)$ es un *grupo* si se cumplen los siguientes axiomas:

(A1) *asociatividad*: dados $x, y, z \in G$, $(x \odot y) \odot z = x \odot (y \odot z)$;

(A2) *identidad*: existe un elemento $e \in G$ tal que e es una identidad de G; es decir, para todo $x \in G$, $x \odot e = x$ y $e \odot x = x$.

(A3) *inversos*: para todo $x \in G$ existe $y \in G$, tal que tanto $x \odot y$ como $y \odot x$ son una identidad de G (a tal y lo llamaremos un *inverso* de x.)

Inverso

Ejemplo 6.17.

(a) La estructura $(\mathbb{Z}, +)$ es un grupo: la suma de enteros es asociativa, el entero 0 es una identidad para la suma y, dado $x \in \mathbb{Z}$, si tomamos a $y = -x$, entonces $x + y = y + x = 0$. Luego todo elemento tiene un inverso. Por ejemplo, un inverso de $x = 4$ es $y = -4$ y un inverso de $x = -5$ es $y = -(-5) = 5$. Un inverso de $x = 0$ es $y = 0$.

(b) La estructura $(\mathbb{N}, +)$ no es un grupo ya que, si bien cumple con los axiomas A1 y A2, no cumple con el axioma A3. Por ejemplo, el elemento $x = 3$ no tiene un inverso $y \in \mathbb{N}$.

(c) La estructura $(\mathbb{Z}, -)$ no es un grupo ya que la operación $-$ no es asociativa. Por ejemplo, $(5 - 4) - 2 = -1$ pero $5 - (4 - 2) = 3$.

(d) Para todo $n \in \mathbb{N}^*$, la estructura $(\mathbb{Z}_n, +)$ es un grupo.

(e) La estructura $(\mathbb{R}^*, \cdot)$ es un grupo: la multiplicación de números reales es asociativa, el número real 1 es una identidad para la operación $\cdot$ y, dado un elemento $x \in \mathbb{R}^*$, si tomamos $y = \frac{1}{x} \in \mathbb{R}^*$, entonces tenemos que $x \cdot y = y \cdot x = 1$. Luego todo elemento tiene un inverso.

(f) Dado $n \in \mathbb{N}$, sea $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$. Es fácil probar que $(n\mathbb{Z}, +)$ es un grupo.

El axioma A2 de la definición de un grupo afirma que todo grupo tiene por lo menos una identidad. Gracias al siguiente teorema podemos concluir que todo grupo tiene una única identidad.

Teorema 6.18 (Unicidad de la identidad en grupos). Sea $(G, \odot)$ un grupo. Dados $e, e' \in G$, si e y e' son identidades con respecto a $\odot$, entonces $e = e'$.

Prueba. Como e es una identidad, en particular, se tiene que e "deja idéntico" a e', esto es, $e \odot e' = e'$. Análogamente como e' es una identidad, en particular, se tiene que e' "deja idéntico" a e. Esto es: $e \odot e' = e$. Entonces concluimos que $e' = e \odot e' = e$, como queríamos. ∎

Sea $(G, \odot)$ un grupo. Por el teorema anterior, existe un único elemento $e \in G$ tal que

$$\forall x \in G : x \odot e = e \odot x = x.$$

Algunos autores suelen denotar a este elemento como 0_G, 1_G o ID_G. Nosotros simplemente lo llamaremos e.

Hemos demostrado que un grupo tiene una única identidad. Ahora demostraremos que en un grupo, cada elemento tiene un único inverso.

Teorema 6.19 (Unicidad de los inversos). Sea $x \in G$ y sean $y, y' \in G$, tales que tanto y como y' son inversos de x; esto es, $x \odot y = y \odot x = e$ y además $x \odot y' = y' \odot x = e$. Entonces $y = y'$.

Prueba. A partir de las hipótesis deducimos que $x \odot y = x \odot y'$. Entonces:

$x \odot y$	$=$	$x \odot y'$	
$y \odot (x \odot y)$	$=$	$y \odot (x \odot y')$	(Operando por y)
$(y \odot x) \odot y$	$=$	$(y \odot x) \odot y'$	(Asoc., A2)
$e \odot y$	$=$	$e \odot y'$	(Hipótesis)
y	$=$	y'.	(e es la identidad de G)

■

Sea $(G, \odot)$ un grupo y sea $x \in G$. Gracias al Axioma A3 y al teorema anterior existe un único $y \in G$ tal que y es una inversa de x. A tal y lo llamaremos x^{-1}. Esto es, x^{-1} es el único elemento en G que verifica que

$$x \odot x^{-1} = x^{-1} \odot x = e.$$

A partir de lo que hemos hecho podemos reformular la definición de un grupo.

Definición 6.20 (Grupo, reformulación). Sea G un conjunto cualquiera y sea $\odot : G \times G \to G$ una operación binaria sobre G. Diremos que la estructura $(G, \odot)$ es un *grupo* si se cumplen los siguientes axiomas:

(A1) *asociatividad*: dados $x, y, z \in G$, $(x \odot y) \odot z = x \odot (y \odot z)$;

(A2) *identidad*: existe un único elemento $e_G \in G$ tal que, para todo $x \in G$, $x \odot e_G = x$ y $e_G \odot x = x$ (a e_G lo llamamos *la identidad de G*);

(A3) *inversos*: para todo $x \in G$ existe un único elemento $x^{-1} \in G$ tal que $x \odot x^{-1} = x^{-1} \odot x = e_G$ (a x^{-1} lo llamaremos *el inverso de x*).

Una observación importante que podemos hacer es que no todos los grupos $(G, \odot)$ verifican que la operación $\odot$ sea conmutativa.

Ejemplo 6.21. Sea $(G, \odot)$ el grupo definido así:

(a) G es el conjunto de todas las biyecciones $f : \mathbb{Z} \to \mathbb{Z}$;

(b) dados $f, g \in G$, $f \odot g := f \circ g \in G$ (operación de composición).

Puede verse que $(G, \odot)$ es un grupo y que además la operación $\odot$ no es conmutativa; por ejemplo, si $f(x) = 2x + 1$ y $g(x) = 3x$, entonces

$$(g \circ f)(x) = g(f(x)) = g(2x + 1) = 6x + 3,$$

$$(f \circ g)(x) = f(g(x)) = f(3x) = 6x + 1,$$

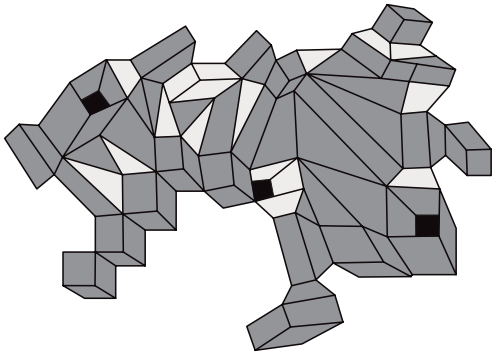
y entonces $f \odot g \neq g \odot f$. En el proyecto propuesto al final de este capítulo se generalizará este ejemplo.

Definición 6.22 (Grupo abeliano). Un grupo $(G, \odot)$ es *abeliano* si la operación $\odot$ es conmutativa, es decir, si se cumple el siguiente axioma: *Grupo abeliano*

(A4) Para $x, y \in G$ se tiene que $x \odot y = y \odot x$.

La mayoría de los grupos que hemos considerado en esta sección son abelianos. Sin embargo, existen grupos no abelianos, por lo cual el axioma A4 no se deduce de los axiomas A1, A2 y A3. Decimos entonces que el axioma A4 es *independiente* de los axiomas A1, A2 y A3, ya que existen grupos abelianos y no abelianos.

Ejercicios



1. Sea $n \in \mathbb{N}^*$. Demuestre que $(\mathbb{Z}_n, +)$ es un grupo.
2. Sea $n \in \mathbb{N}$. Demuestre que $(n\mathbb{Z}, +)$ es un grupo.
3. Demuestre que $(\mathbb{Q}, +)$ es un grupo.
4. Demuestre que $(\mathbb{R}^{>0}, \cdot)$ es un grupo.
5. Demuestre que $(\mathbb{R}^{\geq 1}, \cdot)$ no es un grupo.

6. Sea $(G, \odot)$ un grupo y sean $a, b, c \in G$. Demuestre las siguientes afirmaciones:
   (a) Si $a \odot c = b \odot c$, entonces $a = b$.
   (b) $a \odot a = a$ si y sólo si $a = \text{ID}_G$.
   (c) $a \odot a = \text{ID}_G$ si y sólo si $a = a^{-1}$.
   (d) $(a \odot b)^{-1} = b^{-1} \odot a^{-1}$.
   (e) Si $a = b^{-1}$ entonces $b = a^{-1}$.
   (f) La ecuación $a \odot x = b$ tiene una única solución (en otras palabras, $|\{x \in G : a \odot x = b\}| = 1$).
7. Dé un ejemplo de dos grupos del mismo tamaño que no sean isomorfos entre sí.
8. Dé un ejemplo de un grupo no abeliano que tenga exactamente 24 elementos.

§ 6.3 Isomorfismos entre estructuras

Intuitivamente, dos estructuras matemáticas son isomorfas si, al olvidarnos de los nombres de los elementos de sus conjuntos base, obtenemos estructuras indistinguibles. Dicho de otro modo, dos estructuras son isomorfas si podemos renombrar los objetos de una de las estructuras para obtener *exactamente* la otra estructura (véase la Figura 6.1).

Una *estructura relacional* consiste en un conjunto base A junto con una o varias relaciones sobre A. Una estructura de la forma (A, R) con $R \subseteq A^2$ se llama *grafo dirigido*. Las estructuras consideradas en la Figura 6.1 son grafos dirigidos. Los órdenes parciales son casos especiales de estas estructuras.

Grafo dirigido

Definición 6.23 (Isomorfismo entre grafos dirigidos). Sean (A_1, R_1) y (A_2, R_2) grafos dirigidos. Diremos que f es un *isomorfismo entre* (A_1, R_1) y (A_2, R_2) si f es una función $f : A_1 \to A_2$, tal que

(a) f es biyectiva;
(b) f es un *homomorfismo*; esto es, dados $x, y \in A_1$, xR_1y si y sólo si $f(x) R_2 f(y)$.

Si existe un isomorfismo entre (A_1, R_1) y (A_2, R_2), diremos que estas estructuras son *isomorfas*, lo cual abreviaremos de esta manera:

$$(A_1, R_1) \cong (A_2, R_2).$$

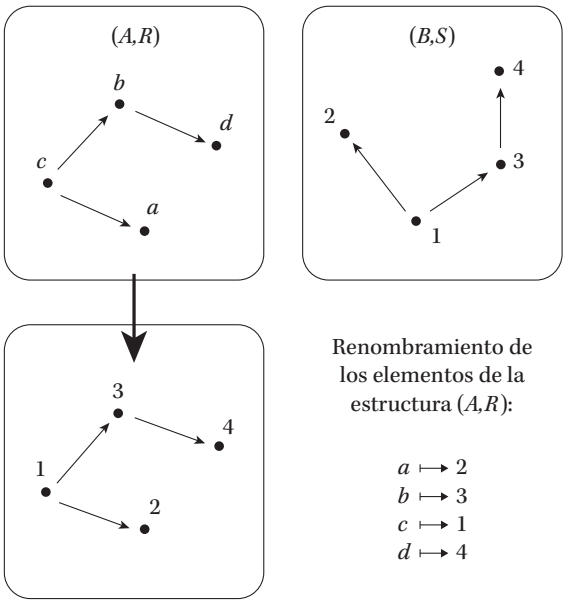


Figura 6.1 : Consideremos las estructuras $(A,R) = (\{a,b,c,d\}, \{(c,a), (c,b), (b,d)\})$ y $(B,S) = (\{1,2,3,4\}, \{(1,2),(1,3),(3,4)\})$. Ellas son distintas. Pero al renombrar los elementos de A obtenemos la estructura de la parte inferior izquierda, $(\{1,2,3,4\}, \{(1,2),(1,3),(3,4)\})$, que es *precisamente* la estructura (B,S). Por ende, (A,R) y (B,S) son isomorfas.

Ejemplo 6.24. Las estructuras $(\mathbb{Z},\leq)$ y $(3\mathbb{Z},\leq)$ son isomorfas. Para ver esto, sea f la función $f : \mathbb{Z} \to 3\mathbb{Z}$ definida por $f(a) = 3a \in 3\mathbb{Z}$, para $a \in \mathbb{Z}$. Veamos que f es un isomorfismo entre $(\mathbb{Z},\leq)$ y $(3\mathbb{Z},\leq)$:

(a) f es una biyección:

  (i) *Inyectividad*: si $f(a) = f(b)$, entonces $3a = 3b$, luego $a = b$.

  (ii) *Sobreyectividad*: sea $y \in 3\mathbb{Z}$. Entonces existe $x \in \mathbb{Z}$ tal que $y = 3x$. Así $y = f(x)$, luego y tiene una preimagen $x \in \mathbb{Z}$.

(b) f es un homomorfismo: sean $a,b \in \mathbb{Z}$. Si $a \leq b$, entonces se tiene que $3a \leq 3b$, dado que multiplicar una desigualdad por un número positivo preserva la desigualdad, y así $f(a) \leq f(b)$. Análogamente podemos demostrar que si $f(a) \leq f(b)$ entonces $a \leq b$. Así que $a \leq b$ si y sólo si $f(a) \leq f(b)$.

Observemos que $\mathbb{Z} \supset 3\mathbb{Z}$. Curiosamente $\mathbb{Z}$ contiene propiamente a un suborden isomorfo. Análogamente puede demostrarse que $6\mathbb{Z} \cong 3\mathbb{Z}$, así que podemos formar una cadena infinita de órdenes, en donde cada uno contiene propiamente al siguiente:

$$\mathbb{Z} \supset 3\mathbb{Z} \supset 6\mathbb{Z} \supset 12\mathbb{Z} \supset \cdots,$$

y *todos* ellos son isomorfos entre sí.

> ☞ **Antes de seguir leyendo**
>
> Demuestre que si $(A_1, \leq_1) \cong (A_2, \leq_2)$ y A_1 tiene un elemento mínimo, entonces A_2 tiene un elemento mínimo. Esto muestra que "tener un elemento mínimo" es una propiedad estructural.

Definición 6.25 (Isomorfismo entre grupos). Sean $(G_1, \odot_1)$ y $(G_2, \odot_2)$ grupos. Diremos que f es un *isomorfismo entre* $(G_1, \odot_1)$ *y* $(G_2, \odot_2)$ si f es una función $f : G_1 \to G_2$, tal que

(a) f es biyectiva;

(b) f es un *homomorfismo*. En otras palabras, dados $x, y \in G_1$, se tiene que $f(x \odot_1 y) = f(x) \odot_2 f(y)$.

Si existe un isomorfismo entre $(G_1, \odot_1)$ y $(G_2, \odot_2)$, diremos que estos grupos son *isomorfos*, y lo abreviaremos así: $(G_1, \odot_1) \cong (G_2, \odot_2)$. Cuando las operaciones $\odot_1$ y $\odot_2$ son claras en el contexto, simplemente escribimos: $G_1 \cong G_2$.

Ejemplo 6.26. Sea $(G, \odot)$ la estructura dada por $G = \{a, b, c\}$, donde a, b y c son elementos distintos, y $\odot$ la operación dada según la siguiente lista:

(i) $a \odot a = c$, $a \odot b = a$, $a \odot c = b$;

(ii) $b \odot a = a$, $b \odot b = b$, $b \odot c = c$;

(iii) $c \odot a = b$, $c \odot b = c$, $c \odot c = a$.

Puede verse que la operación $\odot$ verifica los axiomas A1, A2 y A3 y, por ende, $(G, \odot)$ es un grupo. De hecho, G es isomorfo a $\mathbb{Z}_3$, ya que al cambiar en la anterior lista de operaciones los elementos a, b y c por $[2], [0]$ y $[1]$ respectivamente y la operación $\odot$ por la operación $+$, obtenemos exactamente la lista de la operación de suma en $\mathbb{Z}_3$:

(a) $[2] + [2] = [1]$, $[2] + [0] = [2]$, $[2] + [1] = [0]$,

(b) $[0]+[2]=[2]$, $[0]+[0]=[0]$, $[0]+[1]=[1]$,
(c) $[1]+[2]=[0]$, $[1]+[0]=[1]$, $[1]+[1]=[2]$.

Es decir, la función $f : G \to \mathbb{Z}_3$, dada por $f(a)=[2]$, $f(b)=[0]$ y $f(c)=[1]$, es un isomorfismo entre grupos, ya que es una biyección y, además, para todo $x,y \in G$, $f(x \odot y) = f(x)+f(y)$. Por ejemplo, $a \odot c = b$ y $[2]+[1]=[0]$; por lo tanto,

$$f(a \odot b) = f(b) = [0] = [2]+[1] = f(a)+f(b).$$

Ejemplo 6.27. Consideremos los grupos $(\mathbb{Z},+)$ y $(3\mathbb{Z},+)$. Definimos la función $f : \mathbb{Z} \to 3\mathbb{Z}$ como $f(a) = 3a \in 3\mathbb{Z}$, para $a \in \mathbb{Z}$. Veamos que f es un isomorfismo entre $(\mathbb{Z},+)$ y $(3\mathbb{Z},+)$:

(a) f es una biyección: esto ya lo demostramos en el ejemplo 6.24.
(b) f es un homomorfismo: sean $a,b \in \mathbb{Z}$. Tenemos, por definición, que $f(a+b) = 3(a+b)$, que es igual a $3a+3b$, gracias a la propiedad distributiva de la multiplicación de los números enteros. Pero $3a+3b = f(a)+f(b)$, y así concluimos que

$$f(a+b) = f(a)+f(b).$$

El concepto de isomorfismo entre espacios topológicos es llamado *homeomorfismo*:

Homeomorfismo

Definición 6.28 (Homeomorfismo entre espacios topológicos). Sean (X_1,τ_1) y (X_2,τ_2) espacios topológicos. Diremos que f es un *homeomorfismo* entre (X_1,τ_1) y (X_2,τ_2), si f es una función $f : X_1 \to X_2$ que cumple con las siguientes propiedades:

(a) f es biyectiva;
(b) f "empareja conjuntos abiertos"; es decir, dado $A \subseteq X_1$, tenemos que $A \in \tau_1$ si y sólo si $f[A] \in \tau_2$.

Si existe un homeomorfismo entre los espacios topológicos (X_1,τ_1) y (X_2,τ_2), diremos que estos espacios son *homeomorfos* y lo abreviaremos de esta manera:

$$(X_1,\tau_1) \cong (X_2,\tau_2).$$

Cuando las topologías τ_1 y τ_2 sean claras en el contexto, simplemente escribiremos

$$X_1 \cong X_2.$$

Ejemplo 6.29. Consideremos los espacios topológicos (X_1, τ_1) y (X_2, τ_2), definidos de la siguiente manera:

$$X_1 = \{0,1,2,3\},\ \tau_1 = \{\varnothing, \{1\}, \{3\}, \{1,3\}, \{2,3\}, \{1,2,3\}, X_1\};$$

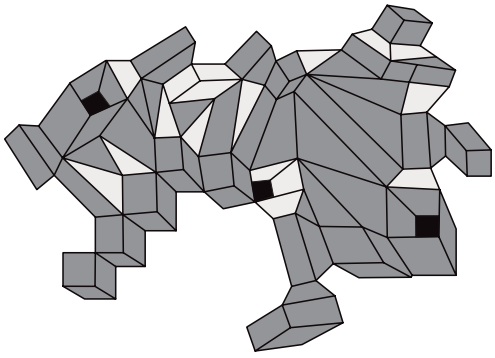
$$X_2 = \{5,6,7,8\},\ \tau_2 = \{\varnothing, \{6\}, \{8\}, \{6,8\}, \{7,8\}, \{6,7,8\}, X_2\}.$$

Para todo $i \in \{1,2\}$ se tiene que (X_i, τ_i) es un espacio topológico (ejercicio 1). Sea $f : X_1 \to X_2$ la función dada por $f(n) = n+5$. Claramente f es una biyección y, para todo $A \subseteq X_1$, se tiene que

$$A \in \tau_1 \text{ si y sólo si } f[A] = \{f(n) : n \in A\} \in \tau_2.$$

Concluimos que f es un homeomorfismo entre espacios topológicos y, por ende, (X_1, τ_1) y (X_2, τ_2) son espacios homeomorfos.

Ejercicios



1. Demuestre que las estructuras definidas en el ejemplo 6.29 son espacios topológicos.
2. Sea $A = \{1,2,3,4\}$. Determine el número de topologías posibles distintas sobre A. ¿Cuáles de ellas son homeomorfas entre sí?
3. Demuestre que $(\mathbb{R}, +) \cong (\mathbb{R}^{>0}, \cdot)$. (*Ayuda*: considere la función dada por $f(x) = e^x$.)
4. Sean $(A_1, \leq_1)$ y $(A_2, \leq_2)$ dos órdenes lineales. Demuestre que si $A_1 \cong A_2$ y A_1 es denso, entonces A_2 es denso. (Un orden parcial $(A, \leq)$ es *denso* si, dados $a, b \in A$, con $a < c$, existe $b \in A$ tal que $a < b < c$.)
5. ¿Son $(\mathbb{Q}, \leq)$ y $(\mathbb{Z}, \leq)$ órdenes isomorfos? Justifique claramente.

6. Sea (A, R) una estructura relacional y sea B un subconjunto propio de A tal que $A \cong B$. Demuestre que existe un conjunto C tal que C es un subconjunto propio de B y $B \cong C$.
7. Sea $A = \{2, 3, 5, 7\}$ y sea D_{210}^+ el conjunto de los divisores positivos de 210. Demuestre que los órdenes $(\mathcal{P}(A), \subseteq)$ y $(D_{210}^+, |)$ son isomorfos. (*Ayuda*: utilice el Teorema 3.29.)
8. Sea $n \in \mathbb{N}^*$, tal que en la factorización por primos de n no aparece ningún primo más de una vez. En otras palabras (utilizando la notación del Teorema 3.27), sea

$$n = \prod_{i=0}^{k} p_i^{\alpha_i},$$

con $k \in \mathbb{N}$ y cada $\alpha_i \in \{0, 1\}$. Consideremos la estructura

$$\mathbb{B}_1 = \{D_n^+, n, 1, \oplus, \odot, \neg\},$$

en donde $a \oplus b := mcm(a, b)$, $a \odot b := mcd(a, b)$, y $\neg(m) = n/m$. Sea $\mathcal{U} = \{i \in \mathbb{N} : 0 \leq i \leq k, \alpha_i = 1\}$. Consideremos la estructura

$$\mathbb{B}_2 = (\mathcal{P}(\mathcal{U}), \mathcal{U}, \varnothing, \cup, \cap, {}^c).$$

Sea $f : D_n^+ \to \mathcal{P}(\mathcal{U})$ la función dada por

$$f(m) = \{i \in \mathbb{N} : p_i \mid m\} \subseteq \mathcal{U}.$$

Demuestre las siguientes afirmaciones:

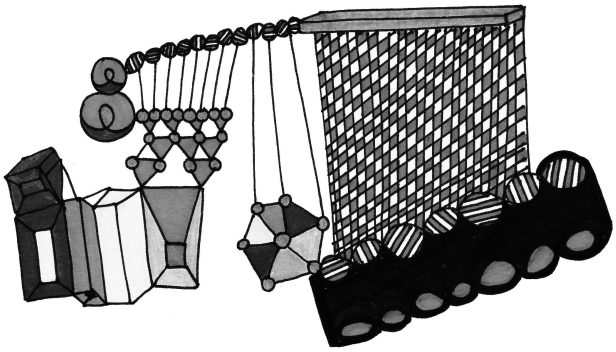
   (a) f es una biyección.
   (b) $f(1) = \varnothing$ y $f(n) = \mathcal{U}$.
   (c) Para $a, b \in D_n^+$, $f(a \odot b) = f(a) \cap f(b)$.
   (d) Para $a, b \in D_n^+$, $f(a \oplus b) = f(a) \cup f(b)$.
   (e) Para $a \in D_n^+$, $f(\neg(a)) = f(a)^c$.
   (f) La operación $\odot$ es asociativa (*Ayuda*: sean $a, b, c \in D_n^+$; como $\mathbb{B}_2$ es un álgebra de Boole, vale que

$$(f(a) \cap f(b)) \cap f(c) = f(a) \cap (f(b) \cap f(c)).$$

   Utilizando (c) y la inyectividad de f demuestre que esto implica que $(a \odot b) \odot c = a \odot (b \odot c)$.)
   (g) La estructura $\mathbb{B}_1$ es un álgebra de Boole.

9. ¿Cómo podría definirse la noción de isomorfismo entre espacios métricos?

Proyecto: Grupos de permutaciones



En este proyecto estudiaremos los llamados *grupos de permutaciones*, es decir, grupos que no son abelianos en general y que fueron una de las motivaciones iniciales para el estudio abstracto de la teoría de grupos. En particular, en este proyecto se demostrará el *Teorema de Cayley*, a saber: para todo grupo G existe un grupo de permutaciones H tal que G es isomorfo a algún subgrupo de H.

Definiciones para referencia

(i) Sea X un conjunto. Una *permutación de* X es un función biyectiva $f : X \to X$.

(ii) Definimos el *grupo de permutaciones o simetrías de* X, y lo simbolizamos $S(X)$, como el grupo de todas las permutaciones de X, en donde la operación de este grupo es la composición de funciones.

(iii) G es un *grupo de permutaciones* si existe un conjunto X tal que $G = S(X)$.

Problemas

1. Sea X un conjunto. Demuestre que $S(X)$ es un grupo.
2. Demuestre que si $|X| = |Y|$, entonces $S(X) \cong S(Y)$.
3. Dado un conjunto X sea $K(X)$ el conjunto de todas las biyecciones $f : X \to X$ que dejan fijos a todos los elementos de X, salvo a un número finito de ellos, es decir, tales que el conjunto
$$\{x \in X : f(x) \neq x\}$$
es finito. Demuestre que $K(X)$ es un subgrupo de $S(X)$.

4. Dado un grupo $(G, \odot)$ y un elemento $g \in G$, definimos el *orden* de g como el mínimo $n \in \mathbb{N}^*$, tal que

$$\underbrace{g \odot g \odot \cdots \odot g}_{n \text{ veces}} = \text{ID}_G.$$

   Si este n no existe, decimos que el orden de g es infinito. Describa en detalle los elementos del grupo $S(X)$ que tienen orden 2, esto es, aquellas funciones f tales que $f \neq \text{ID}_X$ y $f \circ f = \text{ID}_X$.

5. Dado $n \in \mathbb{N}^*$, describa en detalle los elementos del grupo $S(X)$ que tienen orden n. (*Ayuda*: véase el ejercicio 19 de la § 4.4.)

6. Dado $n \in \mathbb{N}^*$, definimos S_n como $S(\{1, 2, \ldots, n\})$. Calcule el grupo S_3 junto con todos sus subgrupos.

7. Sea X un conjunto con n elementos. Demuestre que $S(X)$ tiene $n!$ elementos y que para todo $k \in \mathbb{N}$ con $1 \leq k \leq n$, existe un subgrupo H de $S(X)$ tal que H tiene k elementos.

8. En este ejercicio demostraremos que cualquier grupo es subgrupo de algún grupo de permutaciones. Esto es, para todo grupo G existe un conjunto X tal que G es isomorfo a algún subgrupo de $S(X)$. Este resultado es conocido como el *Teorema de Cayley*.

   (a) Sean G, H grupos y sea $f : G \to H$ un homomorfismo. Demuestre que $\text{IMG}(f)$ es un subgrupo de H.

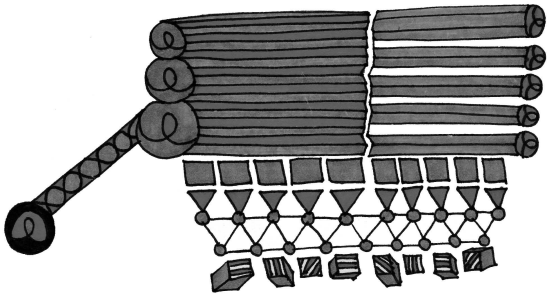
   (b) Dado $g \in G$, sea $\nu_g : G \to G$ la función dada por $\nu_g(h) = gh$ (donde $h \in G$, y gh denota la operación entre g y h en el grupo G). Demuestre que $\nu_g : G \to G$ es una biyección (en otras palabras, que $\nu_g \in S(G)$).

   (c) Dado un grupo G, sea $\nu : G \to S(G)$ la función dada en el literal anterior, la cual le asocia a cada elemento $g \in G$ una biyección $\nu_g : G \to G$. Demuestre que ν es un homomorfismo, es decir, que $\nu(gh) = \nu_g \circ \nu_h$.

   (d) Como ν es un homomorfismo, concluimos que $\text{IMG}(\nu)$ es un subgrupo de $S(G)$. Sea $\sigma : G \to \text{IMG}(\nu)$ la función dada por $\sigma(g) = \nu(g)$. Demuestre que la función σ es un isomorfismo. Esto último garantizará el resultado, pues se tendrá entonces que $G \cong \text{IMG}(\nu)$ e $\text{IMG}(\nu)$ es un subgrupo de $S(G)$.

   (e) Demuestre que en el grupo $\text{IMG}(\nu)$ la única biyección que fija puntos es la identidad. Esto es, para toda $f \in \text{IMG}(\nu)$ tal que $f \neq \text{ID}_G$ se tiene que para todo $x \in G$ $f(x) \neq x$.

Lecturas adicionales

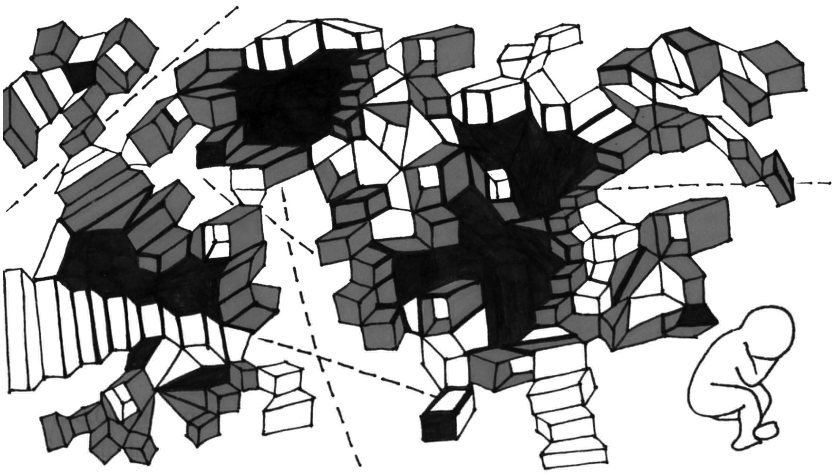


Se recomienda consultar las siguientes lecturas, con miras a profundizar en algunos de los temas tratados en este capítulo:

1. Para más información sobre álgebras de Boole, consulte [2], § 3.4; [6], § 7.3.
2. Para más información sobre espacios métricos, consulte [10], c. 2.
3. Para más información sobre grupos, consulte [3]; [11], § 36.

APÉNDICE A

LÓGICA



En este apéndice vamos a estudiar dos tipos básicos de lógica: la lógica proposicional y la lógica de predicados, también llamada lógica de primer orden. El estudio de ellas servirá para razonar sobre las matemáticas tratadas en este libro.

§ A.1 Lógica proposicional

Una *afirmación* o *proposición* es una expresión del lenguaje que es verdadera o falsa.[1] La afirmación "$x > 5$" es verdadera cuando x es un número mayor que 5, y es falsa de lo contrario.

La lógica proposicional se encarga de estudiar la construcción de afirmaciones a partir de otras utilizando los *conectivos proposicionales* $\wedge, \vee, \neg, \rightarrow$ y $\leftrightarrow$. La razón por la cual se llaman *conectivos* es que unen o conectan dos proposiciones para producir una nueva. La negación $\neg$ es una excepción porque, a partir de una sola proposición, produce otra.

[1] En ese sentido, las preguntas y las órdenes, por ejemplo, no son afirmaciones.

Definición A.1 (Conectivos de la lógica proposicional). Sean a y b proposiciones cualesquiera. A partir de ellas podemos construir las siguientes proposiciones:

Nombre	Símbolo	Se lee:
Conjunción	$a \wedge b$	"a y b"
Disyunción	$a \vee b$	"a o b"
Negación	$\neg a$	"no a" o "no es el caso que a"
Implicación	$a \to b$	"a implica b", "si a entonces b", "b es necesario para a", "a es suficiente para b" o "b, siempre que a"
Equivalencia	$a \leftrightarrow b$	"a si y sólo si b" o "a equivale a b"

Desde temprana edad hemos aprendido el uso *semántico* de los anteriores conectivos, esto es, cómo juzgar la verdad o falsedad de proposiciones donde ellos intervienen. Por ejemplo, sabemos que la proposición "a y b" es verdadera cuando tanto a como b son verdaderas y es falsa de lo contrario, esto es, cuando a es falsa y b es verdadera, a es verdadera y b es falsa, o a y b son falsas. En la tabla de la Figura A.1 resumimos el uso semántico de los distintos conectivos.

a	b	$a \wedge b$	$a \vee b$	$\neg a$	$a \to b$	$a \leftrightarrow b$
0	0	0	0	1	1	1
0	1	0	1	1	1	0
1	0	0	1	0	0	0
1	1	1	1	0	1	1

Figura A.1 : Tabla proposicional de verdad.

En dicha tabla, 0 y 1 corresponden a "falso" y "verdadero", respectivamente. Por ejemplo, la segunda fila establece lo siguiente: si a es falsa y b es verdadera, entonces $a \wedge b$ es falsa, $a \vee b$ es verdadera, etc. Entre tanto, la última columna establece que una equivalencia $a \leftrightarrow b$ será verdadera exclusivamente cuando sus dos partes proposicionales tengan el mismo *valor de verdad*,[2] esto es: o bien ambas verdaderas, o bien ambas falsas. Por ejemplo, la equivalencia "$2 > 3$ si y sólo si todos los animales son leones", es verdadera.

[2] En las lógicas clásicas, el valor de verdad de una afirmación es verdadero o falso. En otras lógicas se consideran valores de verdad adicionales.

Ejemplo A.2. Sea p la afirmación "S es un conjunto finito" y q la afirmación "S es un conjunto con un único elemento". A partir de estas afirmaciones *atómicas*, construimos las siguientes afirmaciones *compuestas*:

$$a := p \wedge q;$$
$$b := p \to q;$$
$$c := \neg q \to p;$$
$$d := q \to p.$$

Hagamos algunas observaciones:

(a) La afirmación a es verdadera o falsa, según S sea finito o infinito. Por ejemplo, si hacemos $S = \{0, 1, 2, \dots\}$, entonces a es falsa.

(b) La afirmación a se puede leer: "Si S es finito, entonces tiene un único elemento". De modo similar, esta afirmación es verdadera o falsa, según sea S.

(c) La afirmación c se puede leer: "Si S no es un conjunto con un único elemento, entonces es finito". Obviamente esta afirmación no es verdadera para todo conjunto S, pues existen conjuntos que no tienen exactamente un elemento, pero que no son finitos.

(d) La afirmación d se lee: "Si S es un conjunto con un único elemento, entonces es finito". Esta afirmación es verdadera para cualquier conjunto S. Notemos que d no afirma que S tiene un solo elemento; afirma que *en caso de* que S tenga un solo elemento, entonces S es finito. La afirmación no se compromete en absoluto en caso de que S no tenga ningún elemento o tenga más de uno.

Definición A.3 (Afirmaciones equivalentes). Diremos que dos proposiciones p y q son *equivalentes* si tienen el mismo valor de verdad. En otras palabras, si una de ellas es verdadera, la otra también lo es y si una de ellas es falsa, la otra también lo es. *Equivalencia*

En matemáticas es frecuente el estudio de afirmaciones equivalentes. Veamos un ejemplo:

Ejemplo A.4. Sea a una afirmación y sean $p := \neg(\neg a)$ y sea $p := a$. Demuestre que p y q son equivalentes.

Solución. Debemos convencernos de que, sin importar si a es falso o verdadero, p y q siempre tienen el mismo valor de verdad. Para esto hacemos una tabla de verdad:

a	$\neg a$	$\neg(\neg a)$	p	q
0	1	0	0	0
1	0	1	1	1

Vemos que si a es falsa, tanto P como Q son falsas, y si a es verdadera, tanto P como Q son verdaderas. En otras palabras, P y Q "tienen la misma tabla de verdad". Luego son equivalentes. ■

El anterior análisis muestra formalmente que negar dos veces una afirmación es equivalente a no haberla negado en absoluto.

Ejemplo A.5. Sea $p := a \to b$ y sea $q := \neg a \vee b$. Demuestre que p y q son equivalentes.

Solución. Lo primero que notamos es que q es $\neg a \vee b$ y no debe confundirse con $\neg(a \vee b)$. Hagamos las tablas de verdad de p y q:

a	b	$\neg a$	$p := a \to b$	$q := \neg a \vee b$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

Como vemos, p y q tienen la misma tabla de verdad. Luego son equivalentes. Por ejemplo, si a es la afirmación "Andrea es alta" y b es la afirmación "Andrea es flaca", entonces las siguientes afirmaciones son equivalentes:

(a) $a \to b$: "Si Andrea es alta, entonces Andrea es flaca".

(b) $\neg a \vee b$: "Andrea no es alta o Andrea es flaca".

Resulta que para cualquier Andrea en que se piense, sea ella flaca o no, y sea alta o no (hay "cuatro posibles Andreas", por así decirlo), las dos afirmaciones anteriores son o ambas ciertas o ambas falsas. Por ejemplo, si Andrea es alta y no es flaca, entonces la implicación $a \to b$ es falsa, como también lo es la disyunción $\neg a \vee b$. ■

§ A.2 La implicación

En general, una afirmación de la forma $p \to q$ se llama una *implicación* y expresa lo siguiente: *Implicación*

(a) si p es verdadera, entonces q también es verdadera; pero

(b) si p es falsa, entonces no se puede concluir nada sobre q.

De este modo, si p es verdadera y q también, entonces $p \to q$ es verdadera. Si p es verdadera y q es falsa, entonces $p \to q$ es falsa. Pero es crucial observar lo siguiente: si p es una afirmación falsa, entonces $p \to q$ será verdadera, *sin importar si q lo sea o no*. Esto ocurre ya que $p \to q$ nos está "diciendo" en esencia lo siguiente:

"Considérame falsa únicamente si p es verdadera y q no lo es".

En la afirmación $p \to q$, p es llamado el *antecedente* y q el *consecuente*. Esto permite expresar el contenido semántico de la implicación, mediante la llamada *Ley del Antecedente Falso*. *Antecedente* *Consecuente*

Observación A.6 (Ley del Antecedente Falso). Considere la implicación $p \to q$. Si el antecedente de la implicación, esto es, p, es falso, entonces $p \to q$ es verdadera. *Ley del Antecedente Falso*

Ejemplo A.7 (Aplicaciones de la Ley del Antecedente Falso).

- La afirmación "Si 2 es impar, entonces 7 es par" es verdadera.
- La afirmación "Si $x \neq x$, entonces $x = x$" es verdadera.
- Supongamos que Carlos es una persona que no tiene hijos. Entonces la afirmación "Todos los hijos de Carlos son orejones" es verdadera. Este ejemplo requiere un poco de análisis. Lo que hay que observar es que la anterior afirmación es la misma que la siguiente: "Para cualquier ser humano h, si h es hijo de Carlos, entonces h es orejón". Esto es,

"Para todo ser humano h, $p \to q$",

en donde $p :=$ "h es hijo de Carlos" y $q :=$ "h es orejón". Dado *cualquier* ser humano h, si p es falso, entonces $p \to q$ es verdadero por la Ley del Antecedente Falso. Para todo h, la implicación $p \to h$ es verdadera, así que "Todo hijo de Carlos es orejón".

Otra manera de convencerse de la verdad de que todos los hijos de Carlos son orejones es preguntarse qué pasaría si no fuera así. Esto es algo natural, pues, si queremos convencernos de que una

afirmación p es verdadera, podemos pensar: supongamos por un instante que la afirmación es falsa. Si a partir de esta suposición llegamos a algo que es contradictorio con la información que tenemos, entonces es porque en realidad la afirmación p es verdadera. Este razonamiento lo hacemos frecuentemente en la vida cotidiana y lo llamamos *razonamiento por contradicción*.

Razonamiento por contradicción

Volviendo a lo anterior, queremos convencernos de que todos los hijos de Carlos son orejones. Razonemos por contradicción, esto es, supongamos que es falso que todos los hijos de Carlos son orejones. Entonces debe existir por lo menos un ser humano h que es hijo de Carlos y que además *no* es orejón. Pero esto es absurdo, puesto que Carlos no tiene hijos. Luego, en particular, tampoco tiene hijos que no son orejones. Hemos llegado a una contradicción con la hipótesis de que Carlos no tiene hijos. Así que necesariamente debe ser cierto que todos los hijos de Carlos son orejones. Esto parece ridículo, pero es verdadero. También todos los hijos de Carlos se llaman Luis y todos los hijos de Carlos hablan 17 idiomas, etc. Todo esto, gracias a la propiedad del antecedente falso.

§ A.3 Demostraciones

Demostración

Una *prueba* o *demostración* es un razonamiento lógico en el que "demostramos", o comprobamos que cierta afirmación es verdadera. Un *teorema* es una afirmación verdadera que tiene una demostración. Uno de los objetivos fundamentales de este libro es que el lector aprenda a demostrar afirmaciones. En esta sección, que puede servir como referencia, se ofrece una guía básica acerca de cómo se puede demostrar una afirmación de acuerdo con su *forma lógica proposicional*, es decir, según si es una negación, disyunción, conjunción, implicación o equivalencia.

Teorema

Observación A.8. Sean a y b proposiciones.

(M1) Para demostrar que $\neg a$ es verdadera, suponga a y razone para concluir una contradicción, esto es, una proposición que siempre es falsa. Una contradicción es una proposición equivalente a una de la forma $p \wedge \neg p$.

(M2) Para demostrar $a \vee b$ puede utilizarse cualquiera de los siguientes métodos:

(M2.1) Suponga $\neg a$ y razone para concluir b.

(M2.2) Suponga $\neg b$ y razone para concluir a.

(M2.3) Suponga $\neg a$ y $\neg b$ y razone para concluir una contradicción.

(M2.4) Razone para concluir a y luego puede afirmar $a \vee b$.

(M2.5) Razone para concluir b y luego puede afirmar $a \vee b$.

(M3) Para demostrar que $a \wedge b$ es verdadera, demuestre *por separado* que a es verdadera y que b es verdadera.

(M4) Para demostrar que $a \to b$ es verdadera pueden utilizarse los siguientes métodos:

(M4.1) Suponga que a es verdadera y razone, utilizando a, para concluir b. En este caso, a se llama la *hipótesis* y b se llama la *conclusión*.

(M4.2) Suponga que $\neg b$ es verdadera y razone para concluir $\neg a$. Este método es llamado el *método de la contrapositiva* o *contrarrecíproca*.

Método de la contrapositiva

(M5) Para demostrar que $a \leftrightarrow b$ es verdadera puede utilizarse cualquiera de los siguientes métodos:

(M5.1) Demuestre por separado $a \to b$ y $b \to a$. Este método es llamado el *método de la doble implicación*.

Método de la doble implicación

(M5.2) Encuentre una afirmación c tal que a y c sean equivalentes y, además, b y c sean equivalentes.

A partir de estos esquemas, los cuales hemos etiquetado por conveniencia, el lector podrá deducir esquemas similares adicionales. Por ejemplo, para probar que a es verdadera, bastaría probar que $\neg(\neg a)$ es verdadera, puesto que a y $\neg(\neg a)$ son equivalentes. Pero para probar que $\neg(\neg a)$, basta probar, por M1, que si suponemos $\neg a$, razonando llegamos a una contradicción. En conclusión, obtenemos el famoso método de la *prueba por contradicción*:

Prueba por contradicción

Observación A.9 (M6, *Método de contradicción*). Para probar una afirmación a, suponemos que es falsa, es decir, suponemos que $\neg a$ es verdadera y razonamos para concluir una contradicción.

La siguiente regla lógica es fundamental para las deducciones y se llama *Modus ponens*:

MP: *Modus ponens*

Principio A.10 (*Modus ponens*, MP). Si a es verdadera y $a \to b$ es verdadera, entonces b es verdadera.

El anterior principio *motiva* el uso de una "flecha" como el símbolo para la implicación. Una implicación nos permite, de ser verdadera, "movernos desde a hacia b", como lo haría un detective que deduce nueva información a partir de información previa ya conocida. El *Modus ponens* es probablemente el instrumento más útil y simple utilizado en las deducciones.

Supongamos que queremos demostrar que $(a \vee b) \to c$. Podríamos suponer entonces que $(a \vee b)$ es verdadera. ¿Pero qué significa esto? Significa que a es verdadera o b es verdadera. En otras palabras, debemos *separar* el razonamiento en dos casos: uno donde supongamos que a es verdadero y otro donde supongamos que b es verdadero. Si en ambos casos somos capaces de razonar para concluir que c es verdadera, entonces habremos mostrado lo que queríamos, esto es, que si alguna de las proposiciones a o b es verdadera, entonces necesariamente c es verdadera.

Este razonamiento se convierte en un método para demostrar un tipo particular de proposiciones, a saber, aquellas de la forma $(a \vee b) \to c$, esto es, donde la hipótesis es una disyunción. Este método es el siguiente:

Demostración por casos.

Observación A.11 (M8, *Demostración por casos*). Para demostrar una afirmación de la forma $(a \vee b) \to c$, demuestre dos proposiciones *por separado*:

$$\text{(a) } a \to c; \qquad \text{(b) } b \to c.$$

Ejemplo A.12. Demostremos que la afirmación $[(\neg b \wedge \neg a) \to b] \to a$ es verdadera.

Solución. Debemos demostrar que la afirmación $[\neg b \wedge (\neg a \to b)]$ implica la afirmación a. Procedemos de este modo:

1. Suponemos que $\neg b \wedge (\neg a \to b)$ es verdadera. A la afirmación que suponemos que es verdadera la llamaremos *hipótesis*.
2. Dicha afirmación es una conjunción ($\wedge$). Luego en realidad tenemos dos hipótesis, a saber:
3. $\neg b$.
4. $\neg a \to b$.

5. Queremos demostrar que a es verdadera. Para esto utilizamos el método de la contradicción. Es decir, suponemos que $\neg a$ es verdadera.
6. Entonces, por los pasos 4 y 5, estamos suponiendo simultáneamente $\neg a$ y $\neg a \to b$. Luego podemos deducir, por MP, que b es verdadera.
7. Hemos llegado a que b y $\neg b$ son ambas verdaderas por los pasos 6 y 3, lo cual es una contradicción.
8. Como hemos llegado a una contradicción, concluimos que a es verdadera, como queríamos. ■

Veamos un ejemplo de un teorema, junto con su demostración:

Teorema A.13. Para todo número real x, x es distinto de 0, si y sólo si $(x^2 > 0)$.

Prueba. Claramente la proposición "x es distinto de 0" es equivalente a la siguiente afirmación:

$$x > 0 \ \vee \ x < 0.$$

Debemos demostrar, entonces, lo siguiente:

$$(x > 0 \vee x < 0) \leftrightarrow (x^2 > 0).$$

Esta proposición es una equivalencia, de modo que podemos utilizar el método de doble implicación (M5.1) y demostrar dos afirmaciones:

(a) $(x > 0 \vee x < 0) \to (x^2 > 0)$.

(b) $(x^2 > 0) \to (x > 0 \vee x < 0)$.

Para demostrar la afirmación (a), ya que la hipótesis es una disyunción, utilizamos el método de la prueba por casos (M8). Por ende, debemos demostrar dos afirmaciones:

(i) si $x > 0$, entonces $x^2 > 0$;

(ii) si $x < 0$, entonces $x^2 > 0$.

Veamos una demostración de la afirmación (i): si $x > 0$, entonces como el multiplicar por un número positivo a ambos lados de una desigualdad no cambia su signo, concluimos que $xx > x(0)$, pero $x(0) = 0$. Luego $x^2 > 0$. La demostración de la afirmación (ii) es similar. Ambas utilizan el método de prueba directa (M4.1). Ahora demostremos la afirmación (b). Supongamos por hipótesis que $x^2 > 0$. Debemos demostrar que $(x > 0 \vee x < 0)$. Como queremos demostrar una disyunción, utilicemos

el método (M2.1): supongamos, por ejemplo, que es falso que $x > 0$. Entonces, o bien $x = 0$, o bien $x < 0$. Pero no puede ser que $x = 0$, pues se tendría que $x^2 = 0^2 = 0$, contradiciendo nuestra hipótesis ($x^2 > 0$). Entonces $x < 0$, como queríamos. ∎

§ A.4 Lógica de predicados

Sea p la siguiente afirmación: "Ana es japonesa mientras que Gabriel no lo es". Con los instrumentos del cálculo proposicional podemos hacer un mejor trabajo de simbolización y no contentarnos con representar esta proposición mediante la sola letra p. Una razón para ello es que en muchos casos necesitamos sistemas de simbolización más ricos para resolver problemas de manera más eficiente. De modo que podemos convenir en que

q := "Ana es japonesa";
r := "Gabriel no es japonés".

Así, "Ana es japonesa mientras que Gabriel no lo es" corresponderá, naturalmente, a la proposición $(q \wedge r)$.

Sin embargo, podemos hacer un mejor trabajo de simbolización. Notemos que q y r son similares estructuralmente: ambas dicen que *alguien* tiene, o no tiene, la *cualidad* de ser japonés. La palabra "alguien" corresponde a la noción más general de individuo u objeto y la palabra "cualidad" hace referencia a la noción general de propiedad o predicado. Si antes nuestro sistema sólo admitía simbolizar proposiciones con letras y las palabras lógicas "no", "y", "o", "entonces", etc., ahora el enfoque es el siguiente: simbolicemos a los individuos y las propiedades con letras, de modo que las proposiciones consistan en combinaciones de ellas, más los conectivos lógicos. Veamos cómo queda la proposición considerada antes:

Simbolizamos los objetos así: g := "Gabriel", a := "Ana", y la propiedad "tener nacionalidad japonesa" por la letra J. Entonces, "Ana es japonesa" se simboliza así: $J(a)$ y "Gabriel es japonés" se simboliza así: $J(g)$.

Como el lector sospechará, "Ana es japonesa mientras que Gabriel no lo es" se simbolizará así: $J(a) \wedge \neg J(g)$. Note el progreso que hemos hecho hasta aquí. Lo clave es lo siguiente: si alguien lee p sin saber qué representa, sólo sabrá que ésta es una afirmación, pero no se revelará nada sobre su estructura o complejidad. Ahora, si alguien lee $(q \wedge r)$, sabrá que esta expresión representa una conjunción, obteniendo de esta forma más información. Por ejemplo, sabrá que quien afirme $(q \wedge r)$ no puede al mismo tiempo afirmar $\neg r$ sin contradecirse. Finalmente, quien

lea $[J(a) \wedge \neg J(g)]$ tiene ahora más información: por ejemplo, sabrá que al menos un individuo tiene la propiedad J, pero no todos; también podrá concluir que los individuos a y g son distintos, etc.

Ahora introducimos la *cuantificación* a nuestro sistema de simbolización. Supongamos que un detective está investigando un crimen. La lista de todos los sospechosos con sus abreviaciones es la siguiente:

$$a_1 := \text{“Felipe”}, \quad a_2 := \text{“Claudia”}, \quad a_3 := \text{“Hermes”},$$
$$a_4 := \text{“Sonya”}, \quad a_5 := \text{“Zeus”}.$$

Supongamos ahora que el detective ha descubierto lo siguiente:

$p :=$ “Al menos un sospechoso abandonó la habitación principal a las 10:30 PM.”

Nos proponemos simbolizar p de manera más precisa con el lenguaje que hemos desarrollado. Veamos qué hacer.

Una posibilidad consiste en primero definir la propiedad A como la propiedad “haber abandonado la habitación principal a las 10:30 PM”. Esto es, dado cualquier individuo x, sea $A(x)$ la proposición “x abandonó la habitación principal a las 10:30 PM”. Entonces p podría simbolizarse de este modo:

$$A(a_1) \vee A(a_2) \vee A(a_3) \vee A(a_4) \vee A(a_5).$$

Existe una forma más compacta de simbolizar la anterior proposición que, sin embargo, requiere introducir un nuevo símbolo. Primero sea S la propiedad “ser sospechoso”. Esto es, para todo x, $S(x)$ es equivalente a la siguiente proposición:

$$x = a_1 \ \vee \ x = a_2 \ \vee \ x = a_3 \ \vee \ x = a_4 \ \vee \ x = a_5.$$

∃: *Cuantificador existencial*

Es claro entonces que p puede expresarse así: “Existe un individuo x tal que x es sospechoso y tiene la propiedad A”. Si utilizamos el símbolo $\exists$ para simbolizar “existe”, entonces podemos simbolizar p así:

$$\exists x : S(x) \wedge A(x).$$

Con lo anterior no queremos decir que exista un *único* x con las propiedades S y A. Es decir, utilizaremos el símbolo $\exists$ para expresar que “existe por lo menos un…”.

El detective continúa indagando el caso y descubre el siguiente hecho: $q :=$ “Todos los sospechosos bebieron vino la noche del crimen”. Note que q es equivalente a “Para todo x, si x es sospechoso, entonces x bebió vino en la noche del crimen". Si simbolizamos con B la propiedad

∀: *Cuantificador universal*

"haber bebido vino la noche del crimen" y utilizamos el símbolo ∀ para simbolizar "para todo", entonces podemos simbolizar q así:

$$\forall x : S(x) \to B(x).$$

Notemos, sin embargo, que q puede también simbolizarse de la siguiente manera, sin utilizar el símbolo ∀:

$$\neg(\exists x : S(x) \wedge \neg B(x)).$$

La anterior proposición se lee así: no es el caso que exista un sospechoso que no haya bebido vino en la noche del crimen. En general, el lector puede convencerse de que toda proposición que utilice ∀ es equivalente a una que no lo utilice.

El siguiente ejemplo ilustra el fenómeno opuesto:

Ejemplo A.14. Sea H una propiedad. Encuentre una afirmación q que sea equivalente a la afirmación $p := \exists x : H(x)$, tal que q no utilice el símbolo ∃.

Solución. p es la afirmación "al menos un individuo tiene la propiedad P". Notamos que p es equivalente a la siguiente afirmación:

"*No* es cierto que para todo x, x *no* tiene la propiedad P",

pues, si p es verdadera, entonces al menos algún individuo tiene la propiedad H. O, lo que es lo mismo:

$$\neg(\forall x : \neg P(x)).$$

Entonces, si $q := \neg(\forall x : \neg P(x))$, se tiene que p y q son afirmaciones equivalentes.

Los símbolos ∃ y ∀ se llaman respectivamente *cuantificador existencial* y *cuantificador universal*.

Definición A.15 (Lógica de primer orden). Las afirmaciones de la lógica de predicados o de primer orden son aquellas que se construyen utilizando los siguientes instrumentos:

(a) los conectivos proposicionales: $\wedge, \vee, \neg, \to, \leftrightarrow$;

(b) el símbolo de igualdad: $=$;

(c) predicados: $P, Q, R, \ldots$;

(d) letras de variables y constantes: $x, y, z, \ldots$; $a, b, c, \ldots$;

(e) los cuantificadores existencial y universal: $\exists, \forall$.

Ejemplo A.16. Sea $P(x)$:="x es periodista", $R(x)$:="x es ruidoso", $A(x,y)$:="x es amigo de y", b ="Berta", e ="Érika". Simbolice en lógica de primer orden las siguientes afirmaciones:

(a) "Érika es una periodista que no es ruidosa".

(b) "Érika y Berta no son amigas".

(c) "Todos los amigos de Érika son ruidosos".

(d) "Todo periodista es ruidoso".

(e) "Berta es amiga de un no periodista cuyos amigos son todos ruidosos".

(f) "Cuando haya dos amigos distintos, alguno de los dos será ruidoso".

(g) "Todo amigo de Berta es amigo de Érika".

(h) "Érika y Berta tienen exactamente los mismos amigos".

(i) "Érika y Berta tienen exactamente los mismos amigos periodistas".

(j) "Erika y Berta no tienen exactamente los mismos amigos".

Solución.

(a) $P(e) \wedge \neg R(e)$.

(b) $\neg A(b,e)$.

(c) $\forall x : A(e,x) \to R(x)$.

(d) $\forall x : P(x) \to R(x)$.

(e) $\exists x : A(b,x) \wedge \neg P(x) \wedge (\forall y : A(x,y) \to R(y))$.

(f) $\forall x,y : ((x \neq y \wedge A(x,y)) \to (R(x) \vee R(y)))$.

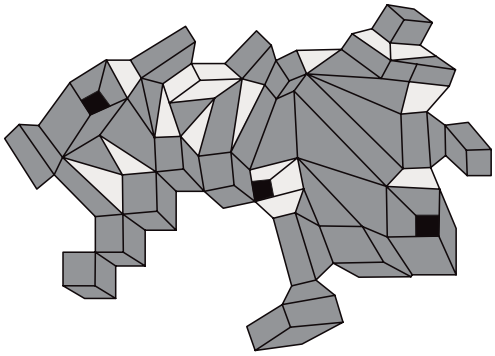
(g) $\forall x : A(b,x) \to A(e,x)$.

(h) $\forall x : A(b,x) \leftrightarrow A(e,x)$.

(i) $\forall x : P(x) \to (A(b,x) \leftrightarrow A(e,x))$.

(j) $(\exists x : A(b,x) \wedge \neg A(e,x)) \vee (\exists x : A(e,x) \wedge \neg A(b,x))$.

Ejercicios

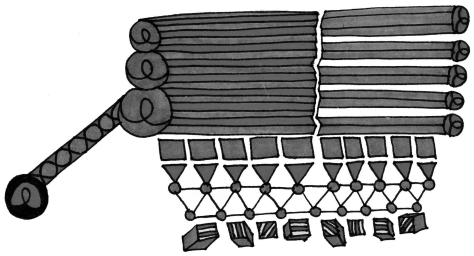


1. Demuestre que las afirmaciones $p := \neg(a \wedge b)$ y $q := \neg a \vee \neg b$ son equivalentes, construyendo simultaneamente sus tablas de verdad. ¿Qué podemos concluir sobre la tabla de verdad de la afirmación $P \leftrightarrow Q$? (Intente responder a esto último sin hacer la tabla de verdad.)
2. Sea $P := a \wedge (a \to b)$, y $Q := b$. ¿son P y Q equivalentes? Justifique claramente su respuesta.
3. Demuestre mediante una tabla de verdad y un razonamiento lógico informal que las siguientes proposiciones son siempre verdaderas:
   (a) $p \to (q \to p)$;
   (b) $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$;
   (c) $(p \wedge q) \to p$;
   (d) $(p \wedge q) \to q$;
   (e) $p \to (q \to (p \wedge q))$;
   (f) $p \to (p \vee q)$;
   (g) $q \to (p \vee q)$;
   (h) $((p \to r) \wedge (q \to r)) \to ((p \vee q) \to r)$;
   (i) $p \to (\neg p \to q)$;
   (j) $(p \to q) \to ((p \to \neg q) \to \neg p)$;
   (k) $(p \to q) \to (\neg q \to \neg p)$;
   (l) $p \vee \neg p$;
   (m) $(p \leftrightarrow q) \to (p \to q)$;
   (n) $(p \leftrightarrow q) \to (q \to p)$;
   (ñ) $(p \to q) \to ((q \to p) \to (p \leftrightarrow q))$.

4. Simbolice en lógica de primer orden las siguientes afirmaciones:
   (a) "Ningún perro ha ido a Venus, pero todos los animales que han ido a Marte son perros". (*Ayuda*: sea $P(x) :=$ "x es perro", $v :=$Venus, $m :=$Marte, $V(x,y) :=$"x ha ido a y".)
   (b) "Todo ser que haya ido a Marte, ha ido a Venus, y tiene un perro que no ha ido a Venus".
   (c) "Todo restaurante japonés es costoso, pero existen restaurantes costosos que no son japoneses".
   (d) "No todos los números enteros son pares".
   (e) "No existen números pares que sean mayores que 7".
5. Los guanacos:
   (a) Simbolice en lógica de primer orden la proposición "Un guanaco es un hombre perezoso y alegre, cuyos amigos son todos guanacos".
   (b) ¿Existen en el mundo hombres guanacos?
   (c) ¿Puede un guanaco tener amigos tristes?
6. Negación de afirmaciones en lógica de primer orden:
   (a) Sea P la afirmación $\forall x : (\exists y : x < y)$. Encuentre una afirmación equivalente a $\neg P$ que comience con un cuantificador existencial.
   (b) Sea P la afirmación $\exists x : (\forall y : y \leq x)$. Encuentre una afirmación equivalente a $\neg P$ que comience con un cuantificador universal.
   (c) Sea P la afirmación $\forall x : \{\exists y : [\forall z : (z > x \to z \geq y)]\}$. Encuentre una afirmación equivalente a $\neg P$ que comience con un cuantificador existencial.
   (d) Sea P la afirmación $\forall x : p(x) \to [q(x) \wedge r(x)]$. Encuentre una afirmación equivalente a $\neg P$ que comience con un cuantificador existencial.
7. Utilice los métodos de la § A.3 para demostrar las siguientes afirmaciones:
   (a) $x > 4 \to x \neq 0$. (*Ayuda*: utilice M4.2.)
   (b) $(a \to b) \leftrightarrow (\neg a \vee b)$.
   (c) $\{[(a \to c) \vee (b \to c)] \wedge \neg c\} \to (\neg a \vee \neg b)$.
   (d) $\neg(a = 3 \vee a = 5) \leftrightarrow (a \neq 3 \wedge a \neq 5)$.
   (e) $(x = 4 \vee x < -5) \to x^2 > 9$.

8. Supongamos que en mi mano tengo cierta cantidad de monedas; todas salvo dos son de 50 pesos, todas salvo dos son de 100 pesos, y todas salvo dos son de 500 pesos. ¿Cuántas monedas tengo en mi mano? Provea dos posibles respuestas a esta pregunta.

Lecturas adicionales



Se recomienda consultar las siguientes lecturas, con miras a profundizar sobre algunos de los temas tratados en este apéndice:

(a) Para más información sobre lógica proposicional, consulte [6], c. 1.

(b) Para más información sobre teoremas y demostraciones, consulte [11], §§ 2–4.

(c) Para una aproximación más formal y teórica a la lógica y demostraciones, consulte [1].

BIBLIOGRAFÍA

[1] Xavier Caicedo, *Elementos de lógica y calculabilidad*, 2 ed., Una Empresa Docente, Bogotá, 1990.

[2] Peter J. Cameron, *Sets, Logic, and Categories*, Springer, London / New York, 1998.

[3] John B. Fraleigh and Victor J. Katz, *A First Course in Abstract Algebra*, 7 ed., Addison-Wesley, Boston, 2003.

[4] Karel Hrbacek and Thomas J. Jech, *Introduction to Set Theory*, M. Dekker, New York, 1999.

[5] Rafael Jiménez, Enrique Gordillo, and Gustavo Rubiano, *Teoría de números para principiantes*, Universidad Nacional de Colombia, Bogotá, 1999.

[6] Richard Johnsonbaugh, *Matemáticas discretas*, Grupo Editorial Iberoamérica, México, 1988.

[7] Elliott Mendelson, *Introduction to Mathematical Logic*, Van Nostrand, Princeton, NJ, 1964.

[8] Hiram Paley and Paul M. Weichsel, *Elements of Abstract and Linear Algebra*, Holt, New York, 1971.

[9] Kenneth A. Ross and Charles R.B. Wright, *Matemáticas discretas*, 2 ed., Prentice-Hall, México, 1990.

[10] Walter Rudin, *Principles of Mathematical Analysis*, 3 ed., McGraw Hill, New York, 1976.

[11] Edward R. Scheinerman, *Matemáticas discretas*, Thomson, México, 2001.

ÍNDICE ANALÍTICO

A

absorción, 29
afirmación, 297
– a. equivalentes, 299
álgebra
– de Boole, 277
– de conjuntos, 41–48, 63
algoritmo
– de Euclides, 119
– de la división, 110–115
antecedente, 301
aplicación, 188
arista, 219
asociatividad, 26
axioma, 275
– A. de Peano, 104
– de separación, 23

B

Bernstein, *cf.* teorema
biyección, *cf.* función
Boole, *cf.* álgebra

C

cálculo
– de predicados, 306–312
– proposicional, 297–300
campo de una relación, 169
Cantor, *cf.* teorema
caracterización, 11
cardinal, 243–273
caso base, 72
Cayley, *cf.* teorema
ciclo, 218
clase
– de congruencia, 141
– de equivalencia, 206
clase-solución, 152
clausura, 122, 162, 179–186
– de una relación, 179
– – reflexiva, 179
– – simétrica, 179
– – transitiva, 180
– en $\mathbb{Z}$, 122
coeficiente, 140
– binomial, 236
combinación lineal, 111
comparabilidad, 66
complemento, 30–34
composición
– de funciones, 191
– de relaciones, 190
conclusión, 5
conectivos proposicionales, 297
congruencia, 138–151
– clase de, 141
conjunción, 298
conjunto, 1–64
– a lo sumo enumerable, 255
– abierto, 279
– agradable, 282
– bien ordenado, 67
– c. comparables, 17
– c. disjuntos, 25
– c. equipotentes, 245
– cerrado, 162, 282
– de índices, 50
– de representantes, 213
– enumerable, 255–264
– finito, 2, 95, 252–255
– hereditario, 282
– igualdad de c., 7–10
– inductivo, 71, 81
– infinito, 2, 95
– linealmente ordenado, 174

– no enumerable, 264–270
– parcialmente ordenado, 16, 175, 276
– potencia, 15–23
– unitario, *cf. singleton*
– vacío, 10–12
conmutatividad, 26
consecuente, 301
constante, *cf.* función
contenencia, 5
conteo, 95–103, 234–240
contradicción, 303
contraejemplo, 30
contrarrecíproca, 303
corolario, 96
cota
– inferior, 175
– superior, 175
cuantificador
– existencial, 10, 308
– universal, 5, 308

D

definición
– buena, 145, 225
– por recursión, 83–90
demostración, 302–306
– por casos, 27, 304
– por contradicción, 303
– por contrapositiva, 303
– por doble implicación, 12, 303
– por doble inclusión, 8
– por elementos, 5
– por inducción, 71–82
– por método directo, 34
diferencia
– de conjuntos, 30
– simétrica, 36, 46
distributividad, 28
disyunción, 298
divisibilidad, 109–164
división, 110–115
divisor, 110
– máximo común d.
– – generalizado, 123
– máximo común d. (MCD), 115–123
dominio de una relación, 169

E

equipotencia, 244
equivalencia, 298
– clase de, 206
– relación de, 205–221, 234–240
espacio
– de Sierpiński, 279
– métrico, 278
– topológico, 279
estructura, 275–296
– de Peano, 104
– linealmente ordenada, 66
– ordenada, 90–95
– relacional, 288
– rígida, 232
– totalmente ordenada, 66
Euclides, *cf.* Algoritmo, *cf.* lema
Euler, *cf.* función
existe, *cf.* cuantificador
extensión, 189
extensional, 4
extensionalidad, *cf.* principio

F

factorial, 83
factorización canónica, 128
Fermat, *cf.* teorema
Fibonacci, *cf.* sucesión
fibra, 199
filtro, 39
función, 165–242
– φ de Euler, 147
– biyectiva, 192–199
– característica, 204
– composición de, 190–192
– constante, 193
– de distancia, 278

– estrictamente creciente, 203
– extensión de, 189
– *identidad*, 187
– invertible, 195
– inyectiva, 192–199
– restricción de, 189
– sobreyectiva, 192–199

G

generalidad, pérdida de, 249
grafo, 219
– conexo, 220
– dirigido, 288
grupo, 283–288
– abeliano, 287

H

Hanoi, torres de, 89
hipótesis, 5
homeomorfismo, 291
homomorfismo, 288

I

ideal, 40, 162, 163
– maximal, 162
– no trivial, 162
– primo, 162, 163
– principal, 162
– propio, 162
idempotencia, 26
identidad, 284
igualdad de conjuntos, 7–10
imagen, 170
– de una función, 199–201
– de una relación, 169
– inversa, 170, 171
implicación, 298, 301–302
– doble, 12
inclusión, 5
inconsistencia, 155
índice, 50–53
inducción, 65–108
– fuerte, 74
– Principio de, 71
ínfimo, 175
intensional, 4
intersección, 23–30
– generalizada, 48–55
inversa
– por derecha, 196
– por izquierda, 196
inverso, 284
inyección, *cf.* función
isomorfismo, 90–95
– entre estructuras, 288–293
– entre estructuras de Peano, 107
– entre grafos dirigidos, 288
– entre grupos, 290

L

lema, 96
– de Euclides, 124
ley
– Cancelativa, 106
– Cancelativa para las Congruencias, 141
– de De Morgan, 44
– de distribución, 28
– del antecedente falso, 11, 301
– l. de complementariedad, 32
– L. de De Morgan, 34
lógica, 297–312
– de predicados, 306–312
– proposicional, 297–300

M

matriz, 240
– booleana, 240
– simétrica, 241
– transpuesta de una, 241
maximal, 175
máximo, 175
minimal, 175
mínimo, 66, 175
Modus ponens, 303

múltiplo, 110
– mínimo común m. (MCM), 137

N

negación, 298
notación
– de corchetes, 2
– de sumatoria, 84
– extensional, 4
– infija, 283
– intensional, 4
– prefija, 283
nulo, 51
número
– entero, 51, 66, 109–164, 222–234
– – construcción de, 222–227
– – módulo *n*, 141–146
– impar, 114
– natural, 4, 65–108
– par, 114
– primo, 124
– – p. relativos, 119
– racional, 51, 222–234
– – construcción de, 232–233
– real, 51

O

operación
– binaria, 283
– entre conjuntos, 23–40
orden, 172–176
– buen, 66–71
– lineal, 17, 66
– parcial, 66, 174
– total, 17, 66

P

par ordenado, 55, 58–59
para todo, *cf.* cuantificador, universal
partes de un conjunto, 18
partición, 209–215
paso inductivo, 72
Peano, *cf.* axioma; estructura
permutación, 217, 294
pertenencia, 2
plano cartesiano, 56, 215
polinomio, 140
potencia de un conjunto, 18
preimagen, 170
– de una función, 199–201
primo, *cf.* número
primos relativos, 119
principio
– de Extensionalidad (PE), 7
– de Inducción (PI), 71
– de Inducción Fuerte (PIF), 74
– del Buen Orden (PBO), 66–71
producto
– booleano, 241
– cartesiano, 55–63
propiedad
– del par ordenado, 59
– dual, 44–45
proposición, *cf.* afirmación
prueba, 302–306

R

recíproco, 141
recursión, 83–90
relación, 165–242
– ⊆, 15–23
– antisimétrica, 172
– asimétrica, 172
– completa, 177
– composición de, 178
– composición de r., 190
– de congruencia, 138
– de equipotencia, 244
– de equivalencia, 205–221, 234–240
– *divide* (|), 110
– *identidad*, 168, 187
– inversa, 171
– irreflexiva, 172

– reflexiva, 172
– simétrica, 172
– transitiva, 172
– vacía, 168
representante, 208
representantes, *cf.* conjunto
residuo, 112
restricción, 189
Russell, Paradoja de, 20–21

S

Schröder, *cf.* teorema
Sierpiński, *cf.* espacio
singleton, 3
sistema
– canónico reducido de residuos, 147
– completo de residuos, 146
– reducido de residuos, 147
subconjunto, 5–7
– propio, 9
subestructura, 276
sucesión, 132
– de Fibonacci, 87, 122
– finalmente nula, 132–137
sumatoria, 84
sumersión, 228, 248
– de $\mathbb{N}$ en $\mathbb{Z}$, 227–232
supremo, 175

T

tabla de verdad, 298
tamaño de un conjunto, 245
teorema, 96
Teorema
– Chino del Residuo (TCR), 151–161
– de Cantor, 266
– de Cantor-Schröder-Bernstein (TCSB), 248–252
– de Cayley, 294, 295
– de De Morgan, 44
– – generalizado, 53
– Fundamental de la Aritmética (TFA), 124–137
– Pequeño T. de Fermat (PTF), 138–151
topología, 279
tricotomía, 175
tupla, 58

U

ultrafiltro, 39
uniconjunto, *cf. singleton*
unión, 23–30
– disjunta, 32
– generalizada, 48–55
universo, 25
uno a uno, *cf.* función, inyectiva

V

vacío, *cf.* conjunto
valor de verdad, 298
variable muda, 85
vecindad, 278
vecino inferior, 15
Venn, diagrama de, 17, 19
vértice, 219

ÍNDICE DE SÍMBOLOS

Lógica

$\leftrightarrow$	Equivalencia ("si y sólo si"), 298
$=$	Igualdad, 308
$\exists$	Cuantificador existencial ("existe"), 307
$\forall$	Cuantificador universal ("para todo"), 308
$\neg$	Negación ("no"), 298
$\rightarrow$	Implicación ("Si... entonces..."), 298
$\vee$	Disyunción ("o"), 298
$\wedge$	Conjunción ("y"), 298

Conjuntos notables

$\mathbb{Q}$	Conjunto de los números racionales, 51
$\mathbb{R}$	Conjunto de los números reales, 51
$\mathbb{Z}$	Conjunto de los números enteros, 51
$\mathcal{U}$	Universo de discurso, 25
$\mathbb{N}$	Conjunto de los números naturales, 4
$\mathbb{N}^*$	Conjunto de los números naturales positivos, 51
$\mathbb{Z}_n$	Conjunto de los enteros módulo n, 144
$\mathcal{P}_n(B)$	Subconjuntos de B con n elementos, 96
$\varnothing$	Conjunto vacío, 10
$\{\}$	Conjunto vacío, 10
A_n	Conjunto canónico de n elementos, 252

Notación de conjuntos

(a, b)	Par ordenado (a, b), 55
$\cap$	Operación intersección, 24
$\cup$	Operación unión, 24
$\mathcal{P}(A)$	Conjunto potencia de A, 18
$\setminus$	Diferencia de conjuntos, 30

$A \times B$	Producto cartesiano, 56
A^2	Producto cartesiano entre A y A, 56
$\bigcap$	Intersección generalizada, 49
$\bigcup$	Unión generalizada, 49
$\in$	Símbolo de pertenencia, 2
$\prod_{i \in I} A_i$	Producto de los A_i, 272
$\subsetneq$	Símbolo de contenencia propia, 9
$\subset$	Símbolo de contenencia propia, 9
$\subseteq$	Símbolo de contenencia, 5
$A \sqcup B$	Unión disjunta de A y B, 271
$A!(k)$	Conjunto de todas las tuplas de A sin repetición, 100
$A \triangle B$	Diferencia simétrica, 36
A^*	Conjunto de elementos no nulos de A, 51
A^+	Conjunto de elementos positivos de A, 51
A^-	Conjunto de elementos negativos de A, 51
$A^{<a}$	Conjunto de elementos de A menores que a, 51
$A^{>a}$	Conjunto de elementos de A mayores que a, 51
$A^{\geq a}$	Conjunto de elementos de A mayores o iguales que a, 51
$A^{\leq a}$	Conjunto de elementos de A menores o iguales que a, 51
^{c}	Operación de complemento, 31

Divisibilidad

(a)	Ideal principal generado por a, 162
(a,b)	Máximo común divisor entre a y b, 116
$\text{CL}(A)$	Clausura de A, 122
$\equiv_n$	Congruencia módulo n, 138
MCD	Máximo común divisor, 123
MCM	Mínimo común múltiplo, 137
$\mid$	Relación *divide*, 110
$\text{RES}_d(a)$	Residuo de a módulo d, 112
$\varphi(n)$	Función φ de Euler, 147
D_a	Conjunto de divisores de a, 115
R_n	Sistema canónico reducido de residuos, 147

Relaciones y funciones

$[a]_E$	Clase de equivalencia de a módulo E, 206
$\circ$	Composición de funciones, 190
$\binom{n}{k}$	Coeficiente binomial, 236
$\text{CMP}(R)$	Campo de una relación, 169
$\cong$	Isomorfismo, 90
$\text{DOM}(R)$	Dominio de una relación, 169
ID_A	La relación identidad sobre A, 168
$\text{IMG}(R)$	Imagen de una relación, 169
$\text{ÍNF}(A)$	Ínfimo de A, 176
$\mapsto$	Símbolo de aplicación de función, 188
$\text{MÁX}(A)$	Máximo de A, 115
$\text{MÍN}(A)$	Mínimo de A, 66
$\overline{R}_{\text{REF}}$	Clausura reflexiva de R, 179
$\overline{R}_{\text{SIM}}$	Clausura simétrica de R, 179
$\overline{R}_{\text{TR}}$	Clausura transitiva de R, 180
$\text{SUP}(A)$	Supremo de A, 176
R^{-1}	Relación inversa, 171
$R^{-1}[A]$	La imagen de A bajo R^{-1}, 171
$R^{-1}[A]$	La preimagen de A bajo R, 171
X/E	Conjunto cociente, 206
$\lvert A\rvert \leq \lvert B\rvert$	Sumersión de A en B, 248
$\lvert X\rvert = \lvert Y\rvert$	Relación de equipotencia, 244

Principios y teoremas notables

PBO	Principio del Buen Orden, 66
PE	Principio de Extensionalidad, 7
PI	Principio de Inducción, 71
PIF	Principio de Inducción Fuerte, 74
PTF	Pequeño Teorema de Fermat, 149
TCR	Teorema Chino del Residuo, 157
TCSB	Teorema de Cantor-Schröder-Bernstein, 249
TFA	Teorema Fundamental de la Aritmética, 125

Otras

$N_\varepsilon(a)$	Vecindad de radio ε centrada en a, 278
$\prod$	Producto generalizado, 127
$\sum$	Notación de sumatoria, 84
$\underline{n}$	Natural n visto como entero, 224
$n!$	n factorial, 83
$S(X)$	Grupo de permutaciones o simetrías de X, 294

Este libro se terminó de imprimir en septiembre de 2009 en los talleres de Kimpres Ltda. Se compuso en LaTeX con la clase `Memoir`, usando los tipos *Kepler*. Cuidó de la edición Nicolás Vaughan.